Universidad Carlos III de Madrid

GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA

ESTUDIO DEL RENDIMIENTO BIOMÉTRICO DE DISPOSITIVOS DE HUELLA DACTILAR

ANÁLISIS DE LA INFLUENCIA DEL TAMAÑO DE LA MUESTRA

Autor: Carlos Hernández Paz

Tutor: Raúl Sánchez Reíllo

Leganés a 27 de Septiembre de 2015

Índice

LISTADO DE ACRÓNIMOS

ANSI	American National Standards Institute (Instituto nacional americano de estándares)
API	Application Programming Interface (Interfaz de aplicación de programa)
APP	Application (Aplicación)
BBDD	Base de datos
C#	C Sharp
DET	Detection Error Tradeoff (Detección de errores de compensación)
DHS	Department of Homeland Security (Departamento de seguridad interior)
FAR	False Accept Rate (Tasa de falsa aceptación)
FBI	Federal Bureau of Investigation (Oficina federal de investigación)
FMR	FaLse Match Rate (Tasa de falsos positivos)
FNMR	False Non-Match Rate (Tasa de falsos negativos)
IAFIS	Integrated Automated Fingerprint Identification System(Sistema de identificación automatico de huella dactilar)
IEC	International Electrotechnical Commission (Comisión electrotécnica internacional)
IR	Identification Rate (Tasa de identificación)
ISO	International Organization for Standardization (Organización internacional de estándares)
NBIS	NIST Biometric Image Software (Aplicación biométrica de imágenes del NIST)
NET	Network (Red de trabajo)
NFIQ	NIST Fingerprint Image Quality (Factor de calidad de la huella del NIST)
NIST	National Institute of Standards and Technology (Instituto nacional de estándares y tecnología)
PC	Personal Computer (Ordenador personal)

PCASYS	Pattern Classification Automation System (Sistema automático de clasificación de patrones)
RFID	Radio Frequency IDentification (Identificación por radiofrecuencia)
ROC	Receiver Operating Characteristic (Característica operativa del receptor)
SMT	Scar Mark & Tattoo (Marcas de cicatrices y tatuajes)
TFG	Trabajo Fin de Grado
USB	Universal Serial Bus (Bus universal en serie)
WPF	Windows Presentation Foundation (Fundación de presentaciones Windows)

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

El cambio incesante de la tecnología a nivel global, la ferviente automatización de todo proceso considerado como un hábito humano, o el crecimiento de la comunicación interpersonal, suponen un gran reto para nuestra generación. En concreto, se hacen necesarias ciertas vías para proteger la información personal o para realizar algunos procesos de forma segura. En este sentido, la biometría, entendida como estudio de métodos automáticos para identificar humanos mediante el reconocimiento de uno o más rasgos en su conducta o rasgos físicos intrínsecos, tiene un papel muy importante.

Existen diferentes modalidades de sistemas biométricos entre los que cabe destacar a la huella dactilar, que cuenta con numerosas aplicaciones. Este trabajo se centra en el análisis de este sistema de reconocimiento biométrico. A pesar de que la biometría basada en huella dactilar ha sido ampliamente estudiada en la literatura, existen algunas cuestiones que requieren un mayor desarrollo. Precisamente, el presente estudio se centra en el análisis de la influencia del tamaño de la muestra, o imagen de la huella, en el rendimiento de este sistema. Para llevarlo a cabo, el trabajo se organiza en dos partes. La primera contiene una parte teórica donde se parte del concepto general de biometría para describir después, de manera particular, la evolución de la huella dactilar como sistema de reconocimiento biométrico. En la segunda parte se analiza la relación entre el tamaño de la imagen de la huella en el rendimiento del sistema. Para llevar a cabo ese análisis se han generado dos aplicaciones. Una primera aplicación se encarga de la obtención de resultados generados tras la comparación de dos imágenes, y una segunda de la obtención de medidas estadísticas de dichos resultados.

Este proceso de generación de resultados se ha producido a través de pruebas con diferentes sensores de huella dactilar. A partir del análisis de los resultados, se observa que el tamaño de la imagen de la huella afecta al rendimiento del sistema. Todo ello, nos permitirá establecer qué sensores son más adecuados para cada uno de los tamaños de la muestra de huella dactilar analizados.

Palabras Clave: Biometría, Huella dactilar, Tamaño de la imagen, Rendimiento.

ABSTRACT

Technological changes, the automatization of most processes and the increasing levels of interpersonal information have implied a revolution nowadays. Specifically, several systems have been created for protecting that information or for guarantee security in the access or use of that information. Then, biometrics plays a crucial role. Specifically, biometrics, referred to metrics related to human characteristics, used to label and describe individuals, allows the creation of different authentication systems.

Nowadays there are different biometric methods, such as those that use fingerprints. Despite the amount of applications with this method, there are some questions that need to be further developed. For example, there is a necessity of exploring aspects related to the size of the image and how it affects to the performance of the system. Precisely, this study is covering this gap and analysis the influence of the size of the sample, or the image of the fingerprint, on the performance of this method. The study is organized in two different parts. On one hand, it starts with a brief theoretical part where biometrics are studied from a general concept to the particular case of fingerprints..On the other hand, it is organized a practical part where the empirical investigation is conducted through the creation of two applications; the first one to handle the analysis of each of the images and the second one used for the obtained of statistics measures of the results.

This generation process has produced results through testing different fingerprint sensors. From the analysis of the results, it is realized that the size of the fingerprint image affects system performance. All this information will allow us to establish which sensors are suited for each samples sizes fingerprint analysis.

Keywords: Biometric, Image size, Fingerprints, Performance.

1. INTRODUCCIÓN

A lo largo de este documento se va a presentar un Trabajo Fin de Grado (TFG) en el que se analiza la influencia del tamaño de la imagen en el rendimiento de sistemas biométricos. En concreto, en un sistema biométrico en la modalidad de huella dactilar. Para ello, se analiza una base de datos de imágenes generada a partir de tres sensores de huella dactilar diferentes. Mediante la utilización de herramientas estadísticas y de procesado de imágenes, se determinará el rendimiento de cada uno de los sensores. Con ello, se establecen algunas recomendaciones sobre qué sensor es el más adecuado para cada uno de los tamaños evaluados.

Este primer punto del trabajo, comenzará explicando la motivación para el desarrollo de este TFG, cuáles son los objetivos pretendidos y el marco regulador que ha condicionado esta investigación. Esta parte se concluye con la identificación de la estructura que seguirá el estudio.

1.1. Motivación

El desarrollo tecnológico ha hecho posible el almacenamiento de datos mediante sistemas informatizados. Ello ha generado la necesidad de crear sistemas capaces de proteger dicha información. Los sistemas de reconocimiento biométrico ayudan a solventar algunas de las vulnerabilidades en seguridad que presentan otros sistemas convencionales. Gracias a que los sistemas biométricos se basan en características únicas e intransferibles, sus índices de seguridad son mayores. De este modo, estos sistemas se han ido implementando paulatinamente en dispositivos electrónicos. En cualquier caso, para poder evaluar su fiabilidad es necesario realizar previamente un estudio del rendimiento de los sistemas.

Así, la principal motivación que ha llevado a realizar este trabajo es el desarrollo de un análisis completo de un sistema de identificación biométrica, basado en huella dactilar, y su rendimiento. Con ello, esta investigación permite conocer más acerca de los sistemas biométricos de identificación y verificación automática. Esta cuestión es especialmente importante dentro del campo de la electrónica puesto que estos sistemas cuentan con una base fundamental de programación y de algoritmos de procesamiento. Además, esta investigación permite estudiar el rendimiento de una tecnología en auge, que se encuentra implementada en multitud de países con diferentes aplicaciones, y que cuenta con una gran cantidad de posibilidades para su perfeccionamiento.

Adicionalmente, como objetivo personal, este trabajo me permite conocer una tecnología que me resultaba aparentemente ajena, observar los problemas derivados de la complejidad del estudio, y establecer vías con las que solucionarlos. . De este modo, con este trabajo he podido aplicar diferentes conceptos y temáticas desarrollados a lo largo de mi formación universitaria.

1.2. Objetivos

El objetivo de este estudio es analizar cómo influye el tamaño de las imágenes de huellas dactilares en el rendimiento de los sistemas de reconocimiento biométricos. Esta investigación, se pretende sumar a aquellos estudios que analizan este tipo de sistema y las posibles vías para su optimización. Adicionalmente, mediante el análisis de nuestros resultados se podrán establecer posibles implicaciones prácticas para el desarrollo de productos y/o aplicaciones.

Para conseguir dichos objetivos se utilizará una base de datos de huellas dactilares recogidas por el Grupo Universitario de Tecnologías de la Identificación. A partir de estos datos, se realizarán comparaciones entre las muestras de 50 usuarios, se obtendrán los resultados y se analizarán. Para llevar a cabo este proceso es necesaria, además, la creación de dos aplicaciones:

- La primera se encarga de la obtención de resultados a partir de realizar una comparación de muestras de huella dactilar con un algoritmo.
- La segunda aplicación recopilará todos los resultados y mediante la aplicación estadística instituirá las diferentes gráficas de resultados para que, posteriormente, se analicen.

En la planificación se han tenido en cuenta:

- La optimización de las aplicaciones: el tiempo de procesado de las aplicaciones debía ser breve.
- La ocupación de recursos: para la obtención de los resultados del análisis, eran necesarios recursos disponibles en el departamento y éstos contaban con un tiempo limitado.

1.3. Marco regulador

A continuación se presenta el marco regulador técnico y legal que ha sido tenido en cuenta para el análisis y obtención de resultados. Se distinguen dos principalmente: la norma International Organization for Standardization (ISO)/ International Electrotechnical Commission(IEC) 19795 y la Ley Orgánica 15/1999

1.3.1. Marco regulador Técnico: Norma ISO/IEC 19795

En esta norma se recogen principalmente las buenas prácticas para el desarrollo de una evaluación biométrica, así como los aspectos fundamentales para planificarlos.

Consta de 7 documentos o partes. Las 4 primeras están completamente estandarizadas y las tres restantes a punto de ser aprobadas. La primera parte denominada *Principles and Frameworks*, se encarga de desarrollar los conceptos principales para alcanzar un mayor rendimiento en la evaluación biométrica. En ella se encuentran protocolos y documentos como: *Best Practices in Testing and Reporting Performance of Biometric Devices*. Además, tiene en cuenta las tasas de error y las tasas de *throughput* o de transferencia para estimar el rendimiento. Igualmente, establece las tres fases principales en la evaluación: reclutamiento, verificación e identificación. Dentro de las

clausulas que forman esta primera parte, también se recogen las buenas prácticas a seguir en la óptima recopilación de datos. En concreto, las siguientes [1]:

- Los usuarios y, por tanto, sus muestras deben ser reales
- Si se ha utilizado un usuario para el ajuste del sistema, éste no debe formar parte de la evaluación
- Los usuarios deben pertenecer a la misma región que donde vaya a estar instalado el sistema.
- El reclutamiento y la verificación deben de estar separados.
- Los usuarios deberán adoptar un comportamiento similar al habitual cuando se dispongan a realizar la prueba.
- Las identidades de los usuarios nunca deben de ser reveladas

1.3.2. Marco regulador legal: Ley Orgánica 15/1999

Para la adquisición de las huellas de cada usuario, así como para su utilización en el presente documento, se ha tenido en cuenta la Ley Orgánica de Protección de Datos 15/1999. Esta ley tiene como objetivo garantizar y proteger los derechos fundamentales de las personas físicas, así como su privacidad e intimidad personal y familiar.

Para el presente estudio ha sido necesario tratar datos y ficheros con un carácter personal, de manera muy estricta y bajo la supervisión del director del trabajo. [2]

1.4. Estructura del documento

A continuación se describe el contenido del presente documento. Comenzará con una breve introducción sobre la biometría, con el fin de que el lector conozca todos los aspectos más importantes de esta tecnología. Aquí se incluirán los tipos de sistemas biométricos, sus etapas, o las ventajas frente a otros sistemas no biométricos convencionales. A continuación, se centra en la evolución del estudio de la huella dactilar. Aquí, se incluirán también ejemplos y aplicaciones de este sistema. La estructura continúa con la explicación de las diferentes herramientas, tanto a nivel físico como a nivel de programación, que han ayudado a la consecución del estudio. Para ello se realizan breves descripciones, tanto de los sensores utilizados para el desarrollo de la evaluación, como de las aplicaciones empleadas y del algoritmo principal del estudio. También se explicará cómo han de clasificarse los diferentes tipos de curvas y gráficos que se obtienen. Además, se describirá cómo ha sido generado el código, hasta su versión final, y los resultados obtenidos a partir de la implementación del mismo. Finalmente, se explicarán las relaciones entre cada una de las pruebas realizadas para cotejar el mejor sistema en relación a su tamaño y calidad e implementarlo en la realidad. El documento termina con un apartado anexo, que resume las horas empleadas y el coste total del proyecto.

2. FUNDAMENTOS TEÓRICOS

En esta parte del documento se presentan los aspectos fundamentales para conocer más en profundidad las tecnologías biométricas. En primer lugar, se establecen los conceptos de biometría y huella dactilar. Aquí, también se expone una breve historia de la biometría, centrándose en la huella dactilar como objeto de estudio. En segundo lugar, se introducen unos pequeños ejemplos sobre el estado actual de la investigación en este campo. Por último, se presenta una de las aplicaciones prácticas, como es la adaptación de la tecnología de reconocimiento dactilar en dispositivos móviles

2.1. Definición de biometría

Se denomina biometría como el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas. Los desarrollos más importantes de esta tecnología parten de la necesidad de ocultar nuestra información personal. Por ello, se asegura que la biometría es base fundamental para el estudio de las tecnologías de la seguridad en la información [3].

Los rasgos, físicos o conductuales, en los que se basan los sistemas biométricos deben presentar algunos requisitos básicos como los siguientes: [4]

- Universalidad: todos los usuarios tienen que contar con la característica.
- Singularidad: la característica a estudiar debe de ser diferente al resto.
- Permanencia: debe permanecer en el tiempo y con condiciones ambientales diversas.
- Colectividad: debe ser almacenable de forma cuantitativa.
- Rendimiento: debe existir una relación positiva entre el rendimiento, y la mejora del sistema.
- Aceptación: el usuario debe aceptarla.
- Resistencia a falsificación: debe ser de difícil imitación, aumentando así la seguridad.

2.1.1. Sistemas biométricos frente a métodos convencionales

Existen numerosos métodos para verificar la identidad, diferentes a los sistemas biométricos. Sin embargo, las características de estos últimos, hacen que resulte beneficioso usarlos en comparación a otros métodos convencionales. A continuación, se repasan sus principales ventajas: [5]

- Posibilidad de robo: la sustracción de un patrón humano es prácticamente imposible. A pesar de que existen métodos para ello, muchos avances se están realizando para que la identificación biométrica vaya en dirección al "Anti-spoofing ".

- Posibilidad de pérdida: la posibilidad de no recordar una contraseña o perder una tarjeta es muy probable, sin embargo variar un rasgo biométrico o perderlo es raramente probable.

- Comodidad: La comodidad de la identificación biométrica suele ser mayor, ya que el usuario no tiene porque memorizar largas contraseñas.

Existen sin embargo algunos aspectos que necesitan una mayor investigación [5]:

- Comparación: el proceso de verificación y comparación de un rasgo biométrico tiene como peculiaridad que cuenta con un mayor tiempo de procesamiento, contrario a una contraseña. A pesar de ello se está consiguiendo contemplar un tiempo de procesamiento menor.

- Prevención frente ataques: dado que la identificación biométrica es una tecnología bastante novedosa existen menos medios para prevenir ataques.

- Efectividad en la autenticación: mientras que efectividad de la autenticación mediante código alfanumérico es plena, la identificación biométrica todavía puede dar lugar a errores.

- Coste de implantación del sistema: el coste de implantar un sistema de contraseña por dígitos es menor que el de implantar un sistema biométrico. Esto se debe al mayor número de sensores y componentes necesarios en éste último.

2.1.2. Tipos de sistemas biométricos

Como se ha comentado ya en varias ocasiones, la biometría es el estudio de métodos automáticos para el reconocimiento de individuos. Dicho reconocimiento se basa en el examen de las características biométricas .Así, se pueden distinguir tres tipos de sistemas biométricos principalmente [6]:

- Biometría estática: es el tipo de biometría que se basa en el reconocimiento de rasgos físicos propios del ente a reconocer. Para ello se buscan rasgos propios de todas las personas, tales como la huella dactilar, la geometría de la cara, el análisis de la retina, etc.

- Biometría dinámica: es el tipo de biometría que se basa en comportamientos particulares de cada usuario. Para este análisis se buscan comportamientos como el patrón de voz, la firma manuscrita, la dinámica del tecleo, etc.

- Biometría multimodal: es el tipo de biometría que combina tanto los rasgos físicos como los de comportamiento.

En la figura 1 se puede observar gráficamente los sistemas de identificación biométricos según se analicen características físicas o de comportamiento.

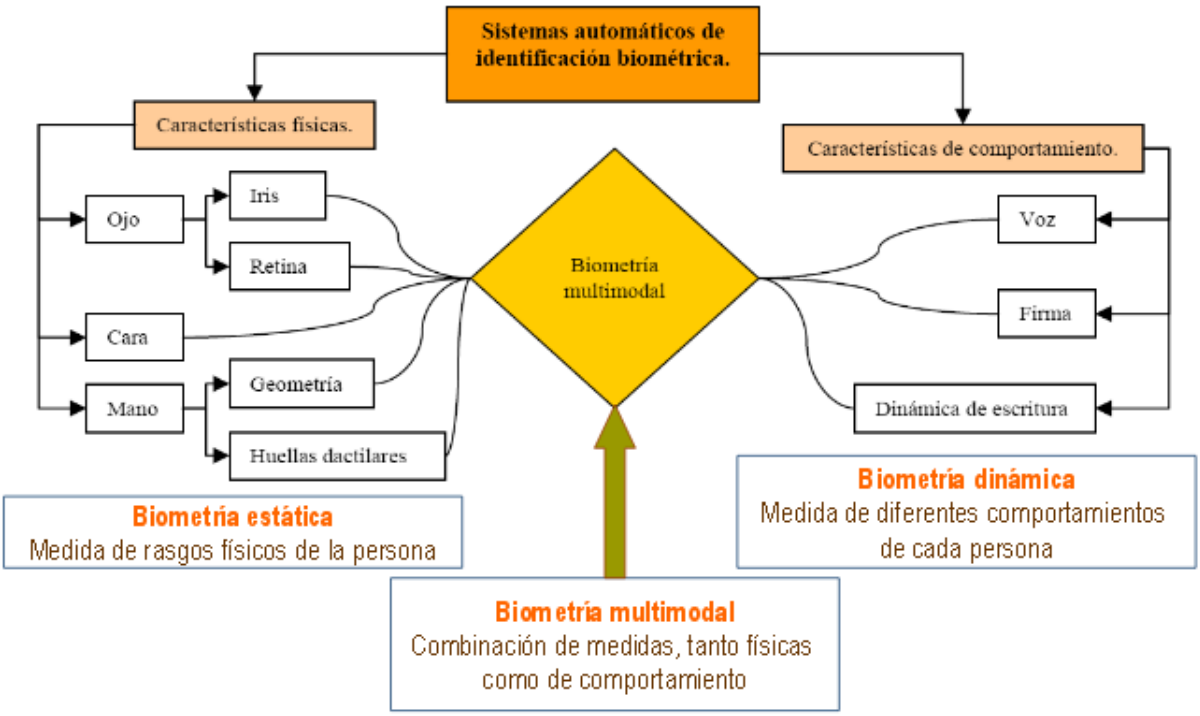

Figura 1. Sistemas automáticos de identificación biométrica [7]

2.1.3. Etapas de un sistema biométrico

A continuación se describe mediante la figura 2 cuáles son las etapas y su secuencia en un sistema biométrico

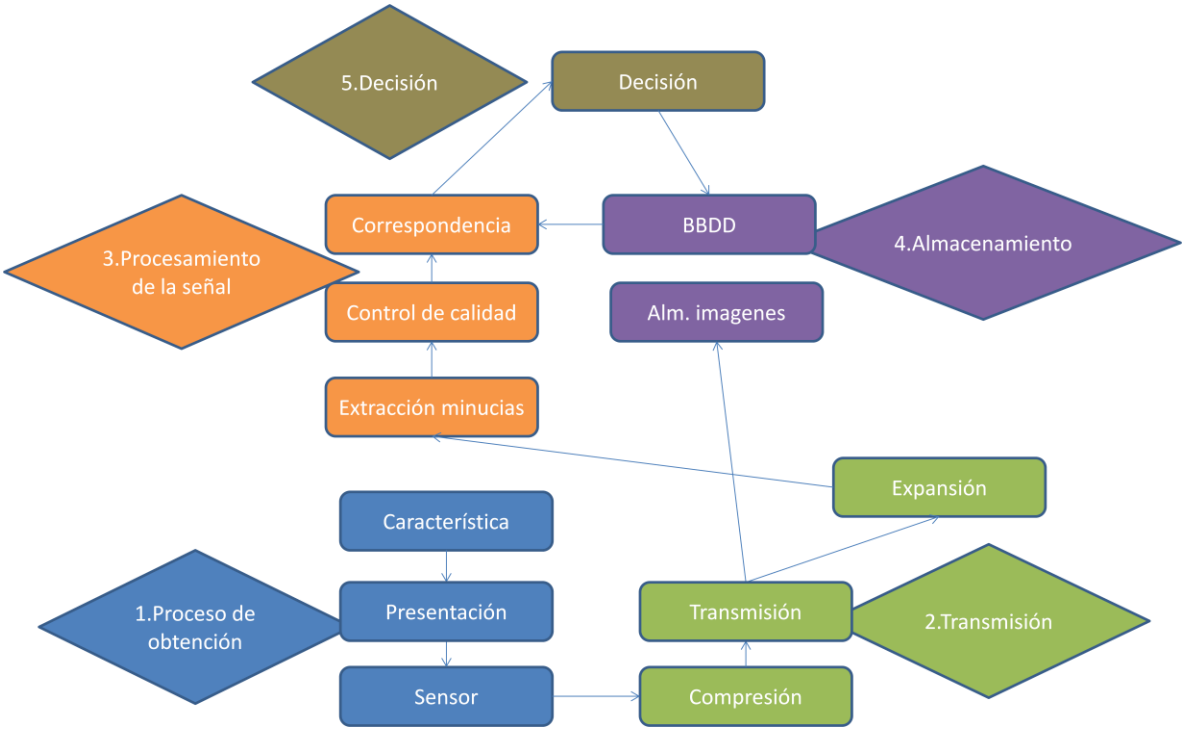

Figura 2.Etapas de un sistema biométrico

2.1.4. Metodología del reconocimiento

La metodología del reconocimiento de los sistemas biométricos está dividida en dos procesos diferentes: verificación e identificación [8].

- Verificación: se trata de un proceso de comparación uno a uno, es decir, el propio usuario es quien determina su identidad. Para ello se toma una muestra de la huella dactilar que se comparara con otra previamente registrada y archivada. Así, si las huellas coinciden, el usuario será verificado y se le proporciona el acceso al contenido.

- Identificación: se trata de un proceso de combinación de uno a muchos. En este caso, el usuario no necesariamente confirma su identidad. La muestra tomada de la huella dactilar se comparará con otras huellas, recopiladas y almacenadas en una base de datos. Cuando se encuentra una combinación positiva, el usuario es identificado, es decir, el sistema encuentra quién es.

2.1.5. Medidas del rendimiento

En todo sistema biométrico es necesario evaluar numerosos aspectos que determinan el rendimiento final del sistema. Una evaluación completa de estos sistemas requiere analizar [9]:

- Rendimiento en la identificación automática de personas.
- Seguridad, integridad y confidencialidad.
- Fiabilidad y mantenimiento
- Aceptación y facilidad de manejo
- Estimación de costes y beneficios

Este estudio se centrará en la evaluación del rendimiento donde se encuentran diferentes tasas de error. Éstas proporcionan una idea sobre la cantidad de errores cometidos en la adquisición y en la comparación. Las principales son:

- False Non-Match Rate (FNMR): es la tasa de error que contempla aquellas pruebas en las que un usuario genuino no ha podido ser verificado a partir de su propia muestra, debido a la no coincidencia en sus características o patrones.

- *False Match Rate* (FMR): esta tasa mide la cantidad de usuarios impostores que han sido verificados como genuinos.

- *False Reject Rate* (FRR): la tasa FRR se compone de todas aquellos intentos que hayan sido incorrectamente denegados.

- *False Accept Rate* (FAR): Con esta tasa se obtiene la cantidad de pruebas de impostor incorrectamente aceptadas. Una prueba puede consistir de uno o más intentos.

- *Error Equal Rate* (EER): es la tasa en la que el ajuste acepta y rechaza los errores. Cuanto más bajo sea, se considera al sistema más exacto. Como se puede observar en la figura3, el EER se puede obtener tras el cruce de la curva FAR y FRR.

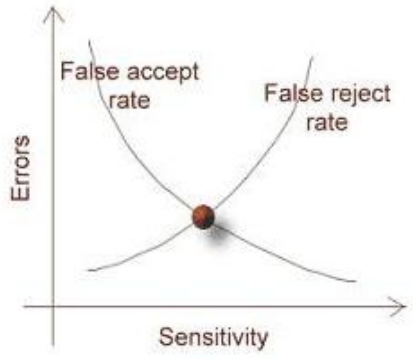

Figura 3. Localización EER [3]

2.2. Definición de huella dactilar

El patrón humano que se analiza en el presente estudio es la huella dactilar. Se conoce como huella dactilar a la impresión visible o moldeada que produce el contacto de crestas papilares de un dedo de la mano. La ciencia que estudia las huellas es la llamada dactiloscopia. Se basa en tres principios fundamentales que enunció Galton, con la clasificación de más de 2632 impresiones dactilares. Los principios son los siguientes:

- Perennidad: las huellas aparecen a partir del sexto mes del desarrollo del embrión y están presentes a lo largo de toda la vida de los seres humanos. Francis Galton en 1892 publicó su libro "*Fingerprint*" donde aseguró que el patrón dactilar del individuo no cambiaba a lo largo de su vida [10].

- Inmutabilidad: las huellas no se ven afectadas por el desarrollo físico o por enfermedades.

- Diversidad infinita: las huellas son únicas e irrepetibles y cuentan con características propias de cada ser humano.

A su vez, Galton determinó las diversas rugosidades localizadas en una huella [11]:

- Papilas: pequeños salientes que nacen en la dermis y sobresalen en la epidermis. Usualmente cuentan con una forma cónica, hemisférica o piramidal.

- Crestas: son los bordes que sobresalen de la piel formados por la sucesión de papilas. Su forma no está realmente definida.

- Surcos: espacios hundidos que se encuentran entre papila y papila.

- Poros: pequeños orificios que se encuentran en la cúspide de crestas papilares o cerca de su vértice. Habitualmente cuentan con formas circulares, ovoidales o triangulares].

Todas las formas y rugosidades crean un dibujo que recibe el nombre de dactilograma. Se localizan tres tipos de dactilogramas diferentes [11]:

- Dactilograma natural: localizado en la yema del dedo, formado por las crestas de manera natural.

  Dactilograma artificial: dibujo que aparece como resultado al entintar un dactilograma natural e imprimirlo en una zona adecuada.

- Dactilograma latente: es la huella dejada por cualquier dactilograma natural al tocar un objeto, queda marcado pero es invisible.

Las minucias o características de Galton son las discontinuidades locales en el patrón de la huella tal y como se muestra en la figura 4. Corresponden normalmente a terminaciones, bifurcaciones o lagunas de la huella dactilar.

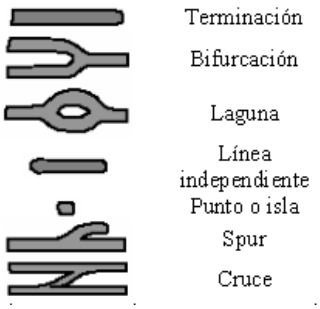

Figura 4.Tipos comunes de minucias [12]

2.3. Historia de la biometría aplicada a la huella dactilar

La biometría basada en la huella dactilar se ha convertido en una tecnología fácilmente adaptable a casi cualquier dispositivo. Su coste en los últimos años ha sido decreciente a la vez que aumentaba su importancia. Este método biométrico ha tenido una enorme evolución a lo largo del tiempo con numerosas aplicaciones que se comentarán más adelante.

Los inicios de la biometría se remontan a finales del siglo XVII de manera reconocida. No obstante, el primer tipo de análisis biométrico se produce mucho tiempo antes, cuando los comerciantes chinos, para distinguir a un niño de un joven, utilizaban la impresión de la palma de la mano y de la huella dactilar [12]. Se reconoce como pionero en el estudio de la huella dactilar al médico italiano Marcello Malpighi, el cual comenzó a estudiar las capas de la piel "*Capa de Malpighi*" así como las crestas, surcos, espirales y lazos localizados en la huella dactilar. Ya a finales del siglo XIX, el D. Henry Faulds retomó la investigación de las huellas dactilares. Además, propuso un método para clasificar dichas huellas y formuló la teoría de la inmutabilidad de las huellas dactilares, donde afirmó que este patrón humano podía suponer un medio para la identificación de individuos en escenas de crímenes. Dos años después, Juan Vucetich fue el primero en esclarecer un crimen, identificando a su autor por medio de las huellas dactilares. Igualmente, en el ámbito de la criminología apareció la figura de Bertillon, creador del sistema antropométrico de Bertillon. Este sistema fue muy utilizado durante unos años. Con él se realizaban mediciones que conseguían identificar al sujeto por diferentes parámetros: altura, estiramiento (anchura de hombro a hombro), busto, longitud y anchura craneal, longitud del oído derecho, longitud del pie izquierdo, longitud del dedo medio izquierdo, longitud del codo izquierdo y la anchura de mejillas.

Sin embargo, el gran avance en la investigación biométrica surgió con la aparición de Francis Galton, tal y como se ha comentado en el punto 2.2 del presente documento, enunciando sus principios fundamentales. Tras la investigación de Galton aparece la figura de Richard Edward Henry, el cual reemplazó la antropometría de Bertillon por la dactiloscopia de Galton. Con la publicación de "*Clasificación y usos de la huella Dactilar*", Henry, trata de exponer el trabajo de Galton, con una finalidad práctica, dando especial relevancia a la comparación de huellas mediante la determinación de minucias [13]. Ya en 1969 y a partir de la intervención del Federal Bureau of Investigation (FBI), se decidió desarrollar un sistema más automatizado que el de aquel momento. Esto se debe a que el registro de una sola persona podía ocupar mucho tiempo. El FBI, en colaboración con el instituto de estándares y tecnología NIST, desarrolló el proceso. El NIST identificó dos cambios clave. El primero

era el de escanear las tarjetas con huellas dactilares y extraer las minucias de cada huella. El segundo cambio era el de comparar y combinar las listas de minucias contra grandes bases de datos de huellas dactilares. En 1975, el FBI desarrolló un escáner de huella dactilar que era el encargado de extraer las minucias usando tecnología capacitiva. Hasta entonces, el sistema se basaba en la identificación de personas. Sin embargo, a partir del desarrollo del algoritmo M40, por parte del NIST, comenzó la búsqueda de éstas. Inicialmente, se seleccionó una pequeña cantidad de imágenes para comparar que fueron verificadas por técnicos humanos. Con el continuo desarrollo tecnológico en la década de los 90 coexistían 5 sistemas diferentes de identificación por huella dactilar repartidos por todo el mundo.

Finalmente, con el desarrollo de la automatización en los procesos y el afán de integrar un sistema de reconocimiento los Estados Unidos crearon el Integrated Automated Fingerprint Identification System (IAFIS), cuyo propósito era el de adquirir huellas dactilares digitales, extraer las minucias y características principales de cada muestra, y generar un algoritmo de comparación entre huellas.

2.3.1. Ejemplos en la actualidad

A continuación se presentan los ejemplos más significativos de la biometría hoy en día.

2.3.1.1. Fecha de huellas

Actualmente la vanguardia de la biometría dactilar ha conseguido algo, que hasta hace muy poco, era prácticamente imposible, y es el determinar la edad de una huella.

La Haya, el instituto médico-legal holandés, ha determinado por continua petición de la policía la antigüedad de las huellas mediante sus componentes. Cuando una persona toca cualquier objeto, deja su huella de manera digital. Dicha huella se compone de sudor, colesterol y demás elementos químicos propios de la piel, y éstos pueden ser analizados. En concreto, determinando el porcentaje de estos factores se puede conocer la antigüedad de dicha huella. A pesar de que el método es muy innovador y bastante preciso, estos componentes no perduran continuamente en el tiempo. Por ello, a los 15 días de posicionar la huella, es más difícil de determinar. [14]

2.3.1.2. Sonnovation tecnología de acceso dactilar

La integración de acceso en dispositivos móviles mediante huella dactilar ha crecido en los últimos años, aunque en dispositivos de gama alta ya lleva varios años estando presente. Sin embargo, el posicionamiento de dicho sensor ha sido un problema desde el comienzo. Hasta ahora, la integración de estos sensores ha dado buenos resultados situándolos en algún botón de acceso o en la parte trasera del dispositivo.

Actualmente, la compañía estadounidense Sonnovation ha anunciado una tecnología que coloca los sensores biométricos ultrasónicos justo debajo del cristal en teléfonos táctiles, a pesar de coexistir dicho sensor con una capa justo encima. Además, un nuevo avance es que afirman que el sensor en condiciones de suciedad también podría estar operativo sin perder precisión [15].

2.4. Adaptación de sensores dactilares a la telefonía móvil

Uno de los objetivos fundamentales de este TFG, tal y como se ha mencionado en el apartado 1.2 de la memoria, es el de analizar el rendimiento e influencia del tamaño de la huella en sistemas biométricos. Esta cuestión es especialmente importante, por ejemplo, en la verificación para el acceso a información contenida en dispositivos móviles. Actualmente, los dispositivos móviles contienen una ingente cantidad de datos acerca de su propietario: correo electrónico, acceso a banca privada, redes sociales, etc. Por tanto, existe la necesidad de ocultar nuestra información personal de manera segura. Así, se pensó en la integración de un sistema biométrico mediante huella dactilar en este tipo de dispositivos.

Con la evolución electrónica se pudieron desarrollar sensores de menor tamaño para su adaptación en terminales móviles, lo que hasta entonces era imposible por el gran tamaño de dichos sensores. En los móviles, la autenticación biométrica por huella dactilar se realiza utilizando el hardware instalado en el terminal y los datos se almacenarán en la memoria del dispositivo, sin necesidad de recurrir a una base de datos externa centralizada. Al inicio de su implantación, los problemas de almacenamiento eran frecuentes, sin embargo hoy en día son inexistentes. Uno de los desarrollos más interesantes es la utilización del móvil como forma de pago, físicamente o de manera on-line. Surge así la necesidad de asegurar dicha información sensible a accesos no autorizados o frente a ataques web que puedan infectar el dispositivo [16].

Figura 5. Integración sensor delantero [16]

Por su innovación, gran capacidad de seguridad y comodidad, todas las compañías están integrando sensores de huella dactilar en sus dispositivos. Muchos de los fabricantes se han decidido incluir el sensor en el lateral del dispositivo, buscando el reconocimiento con un tamaño reducido del área activa del sensor, tal y como se puede observar en la figura 6. Por el contrario, otros optan por la introducción de un sistema de reconocimiento dactilar en el botón delantero o de inicio del dispositivo, con el fin de que resulte cómodo al usuario tal y como se observa en la figura 5.

Figura 6. Integración sensor lateral [17]

Por último, también se está observando la integración de dicho sensor en la parte posterior del dispositivo. Esto se debe a que habitualmente, al tomar el Smartphone, se suele situar el dedo índice próximo a la cámara tal y como se muestra en la figura 7.

Figura 7.Integración sensor trasero [18]

No obstante, a pesar de estos avances se ha observado que existe cierta dificultad para la integración de los sensores en los dispositivos móviles. En concreto, el rendimiento de esta tecnología no es el adecuado, contando con tasas de error demasiado elevadas. Por ello, con este análisis se trata de dar una respuesta a cuál es la mejor relación tamaño/rendimiento para incluir sensores dactilares en dispositivos con espacio limitado.

3. DISEÑO Y ESPECIFICACIONES

En este capítulo de la memoria se presenta el diseño de la aplicación principal que nos permitirá llevar a cabo el análisis del rendimiento del tamaño de la muestra en sistemas biométricos.

Este apartado comienza con un estudio general del funcionamiento de la aplicación. Este diseño general se subdivide considerando todas las herramientas y algoritmos que lo forman, con el propósito de alcanzar un análisis exitoso en este TFG.

3.1. Introducción

A continuación se representa de manera global el diseño establecido en el estudio. Consta de 4 partes o bloques que interactúan entre sí para la generación de los resultados finales.

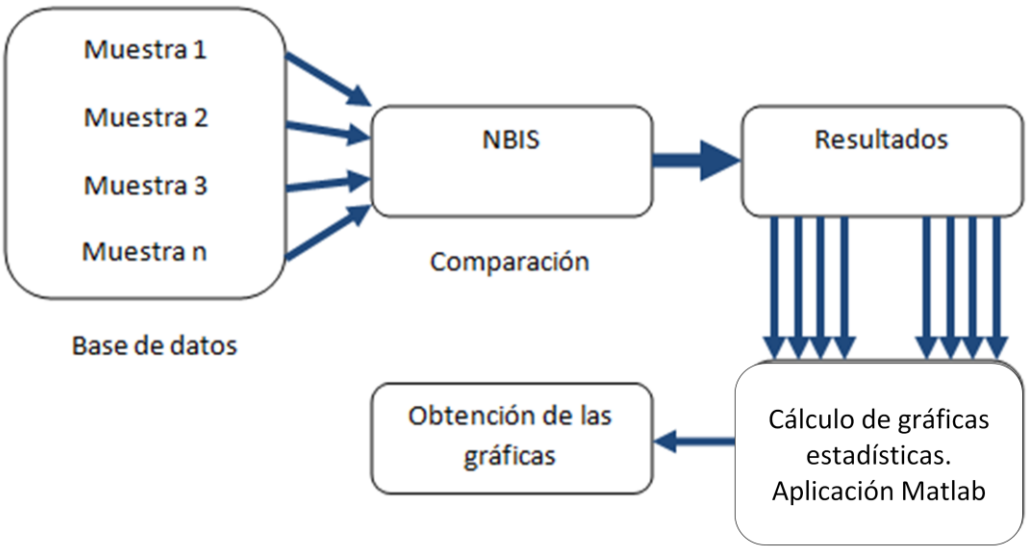

Figura 8. Diseño aplicación biometría

Por un lado, se realizarán nueve pruebas diferentes teniendo en cuenta el factor del tamaño de la imagen, objeto principal en el estudio, así como el tipo de sensor utilizado. Para la realización de las pruebas, tal y como muestra la figura 8, se tomarán inicialmente dos muestras de la base de datos que serán comparadas por el algoritmo NIST Biometric Image Software (NBIS). Hecho esto se obtendrá resultados de comparación que posteriormente serán empleados en la generación de gráficas estadísticas a partir de la herramienta BioSecure Tool.

Las pruebas mencionadas se organizarán según la tabla 1:

Sensor	FULL vs FULL	FULL vs 8x8	8x8 vs 8x8
FPC	Prueba 1	Prueba 2	Prueba 3
NXT	Prueba 4	Prueba 5	Prueba 6
UPK	Prueba 7	Prueba 8	Prueba 9

Tabla 1. Pruebas del estudio

Para llevar a cabo estas pruebas son necesarias diversas herramientas involucradas en el análisis biométrico. Se identifican dos tipos de herramientas en la evaluación, dependiendo de su naturaleza:

- Herramientas físicas: se cuenta con ellas en el laboratorio y se utilizarán principalmente para la captación de huellas (sensor capacitivo *FingerPrint,* otro capacitivo de la marca *Eikon Touch* y uno térmico de la marca *Next).*
- Herramientas lógicas: como es el caso de los dos entornos de desarrollo que nos ayudarán a la obtención de resultados (Visual Studio) o a la generación de gráficas estadísticas (MatLab).

Para la utilización de las herramientas lógicas ha sido necesario desarrollar dos aplicaciones en los distintos entornos previamente mencionados:

- Aplicación de extracción y comparación de las muestras, cuya finalidad es la de obtener los valores de resultado a partir de la extracción de las minucias y su posterior comparación.
- Aplicación estadística, cuyo objetivo era el de proporcionar diversas curvas y valores estadísticos.

El objetivo final del uso de la instrumentación mencionada es el de generar una evaluación veraz que permita conocer la influencia del tamaño de la muestra en el rendimiento del sistema biométrico.

3.2. Herramientas de Partida

A continuación se presentan todas las herramientas y medios necesarios para la llevar a cabo la investigación objeto de estudio en este TFG.

3.2.1. Sensores

Previo al análisis de cada uno de los sensores, se introducen las tecnologías que éstos utilizan para la captación de huellas:

- Sensor capacitivo: el sensor se compone de un circuito integrado de silicio con una superficie llena de transductores. Cada pixel o transductor cuenta con dos electrodos metálicos adyacentes. Cuando el dedo se sitúa sobre la superficie se reduce la capacidad entre los electrodos, los cuales forman la realimentación de un amplificador inversor. Cuantas más irregularidades se detecten, crestas o surcos del dedo, más se reducirá dicha capacidad. Por el contrario, la capacidad aumentará cuanto más espacio localice entre ellas. Habitualmente estos sensores solo trabajan correctamente con pieles sanas y sin durezas. Factores como la humedad, la grasa o el polvo afectarán a su rendimiento.[19]

- Sensor Térmico: para este tipo de sensores, se detecta el calor conducido por el dedo, aumenta cuando hay irregularidades en él y disminuye si encuentra un valle o espacio libre. La innovación en este tipo de sensores nació con el desarrollo del "*Finger Chip"* es decir un circuito integrado al dedo compuesto de silicio y una matriz de píxeles. Cada uno estará cubierto de una capa de material piro eléctrico en el que una variación de la temperatura produce una variación en la distribución de carga en su superficie. Cuenta con una calidad suficiente como para captar huellas en manos desgastadas, con suciedad o grasa.[19]

A continuación se presentan los sensores utilizados para la evaluación.

3.2.1.1. FPC 1011F3 Fingerprint Sensor

Se trata de un sensor de huella basado en tecnología capacitiva. Cuenta con 256 valores en la escala de grises por cada pixel. Su funcionamiento se basa en enviar una señal eléctrica directamente hacia el dedo. Comparando la capacitancia, determinará si hay o no espacio entre las crestas de la huella delimitando así la forma de ésta. Al ser capacitivo permite la implementación de una capa resistente más gruesa por lo que su uso según el fabricante puede ser ilimitado.

Se trata de un sistema robusto y apto para entornos industriales, que cuenta con la capacidad de captar una huella húmeda o sucia. En sí, el sensor cuenta con una guía en su estructura para acomodar el dedo a la superficie, gráficamente representado en la figura 9. Además cuenta con una resolución de 363 dpi. El área de captura de la imagen es de 10,6 x 14mm y el tamaño de la imagen de la huella es de 152x200 pixeles [20].

Figura 9.Representación gráfica FPC 1011F3 [20]

3.2.1.2. NB – 3010 - U Fingerprint sensor

El sensor NB-3010-U Fingerprint utiliza la tecnología térmica para la captación de la huella. Tiene una resolución de 385 dpi, y a su vez cuenta con un formato de 256 posiciones en la escala de grises. El tiempo estimado de captación de la huella es de 0,45s, sin embargo, contabilizando el tiempo de identificación se aproxima al segundo. El tamaño de la imagen de huella es de 180 x 256 pixeles, con un área de captura de 11,9x16, 9 mm.

Cuenta con un diseño ergonómico especialmente diseñado para un ordenador personal (PC) por su conexión Universal Serial Bus (USB) 2.0, tal y como se muestra en la figura 10. Su comportamiento

como sensor térmico le permite captar la imagen de la huella mediante la determinación de las pequeñas variaciones de temperatura en ésta. En cuanto a sus condiciones mecánicas, asegura más de 1 millón de reconocimientos [21]

Figura 10.Representación gráfica NB -3010-U [21]

3.2.1.3. EIKON Touch 500 Sensor

Se trata de un sensor de huella dactilar que cuenta con tecnología capacitiva. Se trata de un sensor robusto, de diseño ergonómico con guía para el posicionamiento del dedo para facilitar su utilización al usuario, representado en la figura 11. Muy útil en entornos industriales y bajo situaciones adversas de suciedad o polvo. Cuenta con una resolución de 508 dpi, un área de captura de imagen de 12,8 x 18 mm y un tamaño de imagen de huella de 192 x 270 píxeles. [22]

Figura 11. Representación gráfica EIKON Touch 500 [22]

3.2.2. Base de datos

Antes de pasar a describir la implementación de la aplicación encargada de la comparación y de los resultados obtenidos, se describe la base de datos. Se ha generado una base de datos de huellas con los sensores descritos en el punto 3.2.1 de la presente memoria. La base de datos está formada por 50 usuarios. Su disposición ha sido la siguiente:

- Organización de base de datos (BBDD) TFG Cropped
- Creación de subcarpetas dependiendo del tipo de sensor a utilizar
- Subcarpetas contenedoras según tamaño 8x8 o Full.
- Carpetas de 50 usuarios de cada sensor, con el tamaño de imagen seleccionado.

Situándonos en la posición final de usuario, se recorrerá el camino trazado por la figura 12.

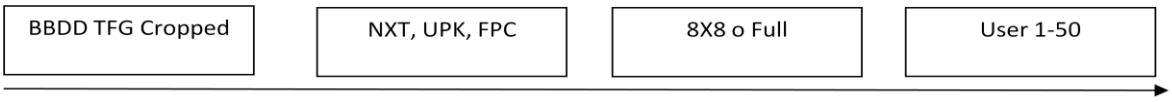

Figura 12. Carpetas para acceder a las imágenes

Por carpeta de usuario se localizan multitud de imágenes, las cuales dependiendo de su título podrán diferenciarse entre verificación y reclutamiento tal y como se expone en la figura 13.

Primera imagen (Reclutamiento)	D:\BBDD-TFG-Cropped\FPC\8x8\100001\FPC-100001-EN-01-02-3.bmp
Segunda imagen (Verificación)	D:\BBDD-TFG-Cropped\FPC\8x8\100001\FPC-100001-V2-02-05-3.bmp

Figura 13.Rutas de acceso a imágenes

La primera imagen a comparar o de reclutamiento se organiza tal y como se comentaba anteriormente. El título en el caso del reclutamiento:

FPC-100001-EN-01-02-3.bmp

- FPC : Tipo de sensor utilizado en la comparación
- 100001: Usuario actual
- EN: Tipo de imagen de “Enrol” o Reclutamiento, es decir imagen a comparar
- 01: Dedo a utilizar
- 02: Intento
- 3: Nivel de Calidad

Por otro lado para el caso de la verificación:

- V*: será el número de visita del dedo seleccionado por parte del usuario

La base de datos inicial era de 582 usuarios. En este TFG se ha reducido el tamaño a 50 usuarios, debido a la enorme cantidad de tiempo que llevaría su procesado. Con ello, se reduce la resolución de las gráficas estadísticas pero no su calidad. La optimización y generación de la base de datos ha sido muy útil para poder obtener los resultados de las comparaciones de manera rápida y de forma intuitiva. Así, se ha podido simplificar el código implementado en la aplicación de comparación desarrollada en el punto 4.1 del presente documento.

3.2.3. Algoritmos de procesado y comparación

3.2.3.1. MINDTCT

Este detector de minucias cuenta con un diseño modular y dinámico. El funcionamiento de este algoritmo se representa en la figura14:

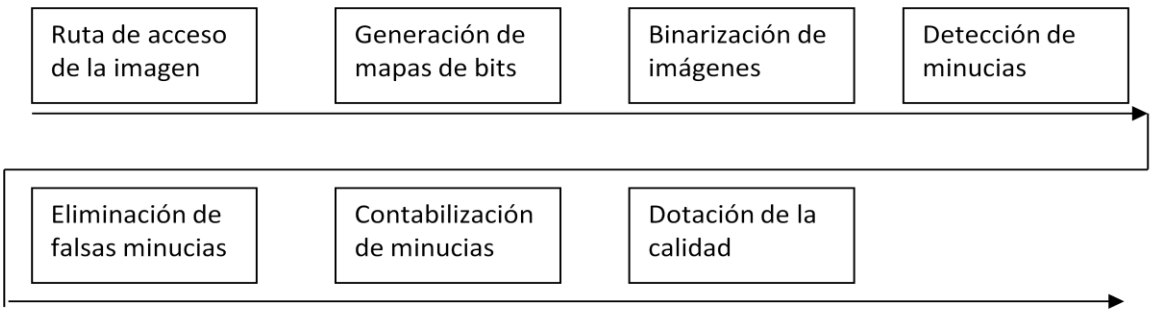

Figura 14.Funcionamiento Algoritmo MINDTCT

1- La primera parte del algoritmo se encarga del acceso a la imagen mediante la ruta configurada. Cuenta con los siguientes formatos de lectura WSQ, JPEGB, JPEGL, IHEAD, así como Instituto nacional americano de estándares (ANSI) o NIST. MINDTCT cuenta con una opción que permite trabajar imágenes con bajos contrastes.

2- En ocasiones la imagen de la huella varía, especialmente en el caso de huellas latentes, es decir, aquellas en las que determinadas áreas puedan estar dañadas, como es el caso de las huellas con bajos contrates (figura 15), bajo afluente de bifurcaciones (figura 16) o minucias y alta curvatura (figura 17).

Figura 15.Bajo contraste [23]

Figura 16.Bajas bifurcaciones [23]

Figura 17.Alta curvatura [23]

Finalmente, una vez eliminados todas estas áreas dañadas, se clasifica la imagen delimitando un conjunto de valores de cada área de la muestra. Se representa en las figuras 18 y 19.

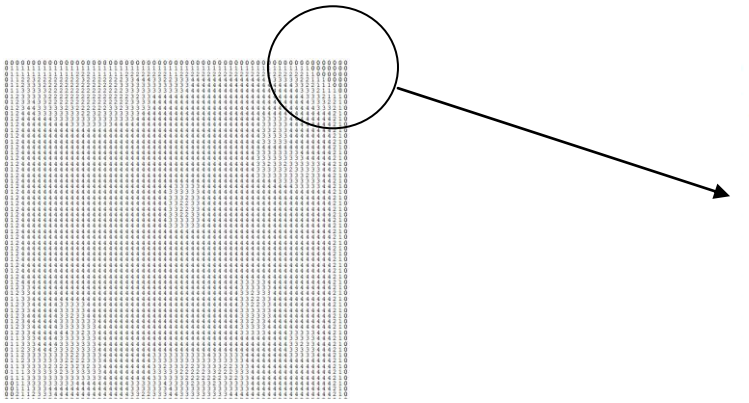

Figura 19. Clasificación de la imagen [23]

Figura 18. Ampliación Figura 19 [23]

3- El algoritmo de detección en este sistema está diseñado para operar a un nivel binario, donde los píxeles negros representan crestas y los blancos valles. Para la creación de la imagen, cada pixel en la escala de grises de entrada debe ser analizada y procesada para determinar si es un pixel blanco o negro. Por cada pixel se asigna un valor binario basado en la dirección de la cresta. En caso de no ser detectada será establecida como blanco. En la figura 20 se puede observar el estado anterior a cualquier proceso y en la figura 21 su estado una vez aplicados los filtros específicos.

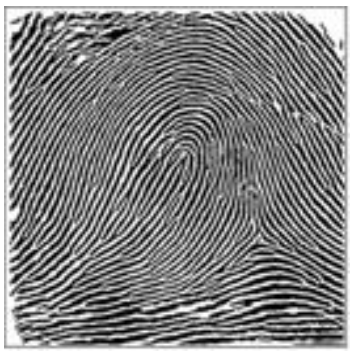

Figura 20. Huella a posteriori [23]

Figura 21.Huella antes de los filtros [23]

4- La detección de minucias se realiza mediante patrones predeterminados en una matriz. Es decir, un conjunto de píxeles del patrón seleccionado se compara con unas muestras predefinidas y se evalúa a qué pertenece cada patrón. Las más frecuentes son las que se encuentran ilustradas en la figura 22.

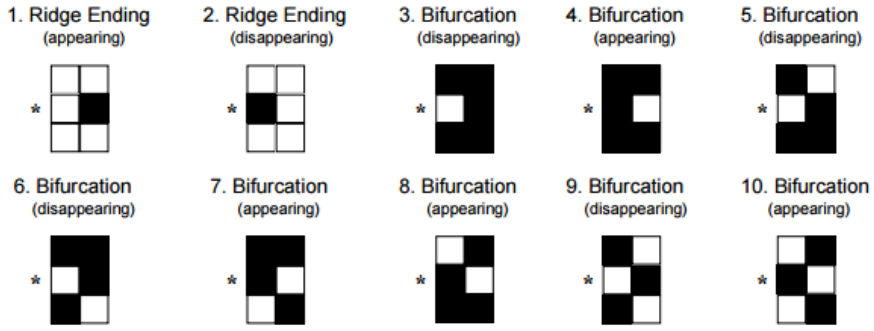

Figura 22.Tipos comunes de patrones en pixeles de una huella [23]

5- La eliminación de falsas minucias se produce cuando un candidato seleccionado, al ser comparado con uno de los patrones, no coincide exactamente y son rechazados.

6- A partir de la creación del patrón y ser comparada una imagen con otra, mediante la función Matcher, se puede determinar el grado de similitud de una respecto a la otra.

7- Con la comparación ya establecida, se genera la calidad de la minucia en la imagen.[23]

3.2.3.2. BOZORTH3

El BOZORTH3 es un algoritmo cuya utilidad es la de tomar las características extraídas de dos huellas dactilares y compararlas, uno a uno o uno a varios. Para realizar esta comparación el algoritmo debe de tener en cuenta varios parámetros de la huella dactilar. En concreto, características representadas por su localización en los ejes de coordenadas (x,y) así como de su orientación (t), generando un modelo de característica delimitado por los puntos (x,y,t). El algoritmo está diseñado para ser invariante a movimientos de la huella, ya sean de traslación o rotación.

El algoritmo se compone de dos grandes fases:

- Primera fase: comparación de características dentro de una huella, cuenta con unas características únicas localizadas en su espacio activo. Las características se sitúan a una distancia relativa las unas de las otras. Dicha medida será invariante para cualquier captación de la huella, figura 23. Este método se encargará de obtener las medidas relativas de todas las características de una misma muestra, almacenarlas en una tabla de comparación y posteriormente compararlas consigo misma. Si la distancia varía no se estará ante la misma muestra [24].

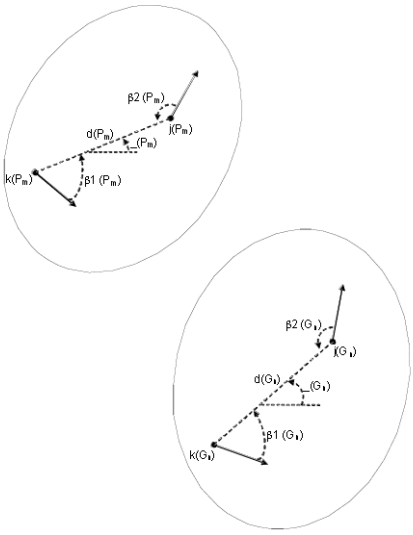

Figura 23. Distancia entre minucias [24]

- Segunda fase: comparación entre distintas huellas, en este caso a contrario que en la primera fase, el algoritmo toma dos huellas diferentes, genera dos tablas de distancias relativas, comparando la compatibilidad en la asociación de dos pares de minucias, generándose un punto de unión entre ellas. El objetivo de esta segunda fase es el de conseguir demostrar si dos huellas diferentes coinciden.

3.2.4. BioSecure Tool

La herramienta BioSecure Tool, muestra las curvas que representan gráficamente las medidas de rendimiento mencionadas en el punto 2.1.5, aportando algunos valores necesarios para realizar la evaluación de un sistema biométrico. Con el fin de verificar un sistema biométrico, este algoritmo se basa en cuatro criterios, dos curvas y dos valores: [25]

- Curva Receiver Operating Characteristic (ROC): representa el porcentaje de intentos impostores que han sido aceptados (FAR) en el eje x, respecto al porcentaje de intentos genuinos aceptados (FRR) en el eje y. Esta curva permite comparar diferentes sistemas bajo las mismas condiciones.

- Curva detection error tradeoff (DET): la curva DET muestra los porcentajes de error en ambos ejes. FAR en el eje x frente a FRR en el eje y usando una escala de desviación normal, lo que facilita su comprensión.

- Valor EER: la aplicación muestra el porcentaje de igual error como el punto donde el FAR es igual al FRR.

- Operating point (OP): en la práctica, los sistemas biométricos operan con un bajo FAR para proporcionar una alta seguridad. Este punto de operación se define como los valores de FRR (%) alcanzados para un FAR fijado. El valor fijado de alpha del FAR depende del nivel de seguridad que requiere el sistema.

3.2.5. Plataformas de desarrollo

A continuación se describen los aspectos más importantes de las principales plataformas de desarrollo.

3.2.5.1. Visual Studio

Para la implementación del algoritmo de comparación y para obtener los resultados de cada una de las imágenes, se ha utilizado el entorno de programación Visual Studio 2013.

Este entorno es el utilizado por sistemas operativos Windows. Soporta multitud de lenguajes de programación y en concreto, el utilizado para este estudio: C Sharp (C#). Permite crear aplicaciones a los desarrolladores así como sitios y servicios web en cualquier entorno que soporte la plataforma .network (.NET), Esto facilita la comunicación entre estaciones de trabajo, páginas web, dispositivos móviles, etc. [26].

3.2.5.1.1. C Sharp (C#)

C Sharp es un lenguaje de programación orientado a objetos cuyo desarrollo y estandarización corrieron por cuenta de Microsoft. Fue diseñado como un lenguaje común en plataforma .NET. Combina la sintaxis básica del lenguaje C/C++ utilizando el modelo de objetos de Java.

La plataforma .NET funciona como una interfaz de programación de aplicaciones Application Programming Interface (API).Cuenta con un conjunto de funciones y métodos que ofrecen las diferentes bibliotecas que pueden añadirse con el fin de ser utilizado por otro software como una capa de abstracción. C Sharp está diseñado para generar programas sobre dicha plataforma [27].

3.2.5.2. MATLAB

MATLAB es un software matemático útil en la manipulación de matrices, la representación de datos y funciones, la generación y uso de algoritmos, la creación de interfaces de usuario y la comunicación con programas de distinto lenguaje.

MATLAB ofrece un entorno de desarrollo integrado (IDE), mediante el uso de un lenguaje de programación propio. Su cálculo numérico está diseñado para trabajar en el entorno de matrices. Por ello, la mayoría de los algoritmos se generan partiendo de vectores y matrices. Además este Software contiene más de 35 funcionalidades agrupadas en paquetes para Simulink [28].

3.3. Especificaciones

3.3.1. Aplicación de procesado

Para la evaluación de resultado se ha utilizado el NBIS. El desarrollo y distribución del NBIS nació a partir de las peticiones del FBI "Federal Bureau of Investigation" y el Department of Homeland Security (DHS). Este software ha sido creado por empleados del gobierno estadounidense, con el fin de distribuirlo de manera gratuita y sin licencias. Cuenta con 8 categorías diferentes:[29]

- Implementación del ANSI/NIST-ITL 1-2007 "Data Format for the Interchange of Fingerprint, Facial, Scar Mark & Tattoo (SMT) Information". Dicho estándar incluye herramientas capaces de leer, escribir, editar y manipular el formato de los ficheros.

- Algoritmo para determinar el NIST Fingerprint Image Quality (NFIQ) de una imagen o valor de ésta. Va desde 1 a 5.

- Desarrollo de un entorno neuronal basado en la clasificación de patrones (PCASYS). Este entorno genera una categorización de la huella teniendo en cuenta diferentes factores como el arco de ésta, la cantidad de vueltas de las crestas reproducidas, etc.

- El detector de minucias "MINDTCT" localiza y guarda todos los finales de crestas y bifurcaciones de la imagen de la huella, tal y como se ha presentado en el punto 3.2.3.1 del presente estudio.

- Herramientas generales para el procesado de imágenes o "IMGTOOLS"

- Un algoritmo de comparación "BOZOTH3" de minucias. Se encargará de comparar tanto de forma uno a uno como uno a varios, tal y como se ha descrito en el punto 3.2.3.2. Acepta minucias generadas por el algoritmo MINDTCT.

- Un algoritmo de segmentación o "NFSEG" capaz de dividir una huella en diferentes imágenes de ésta. Incluso es capaz de eliminar los espacios blancos de una huella.

- Por último el NBIS incluye un espectro de validación y verificación para imágenes de huellas.

3.3.1.1. Diagrama lógico de la aplicación de procesado

A continuación, en la figura 24 se describe un diagrama que representa la lógica seguida por el algoritmo de comparación para la obtención de resultados y su almacenamiento. Los datos de entrada de esta aplicación, son dos rutas de imágenes cuya localización depende del sensor utilizado y del tamaño. Como dato de salida se obtendrá un resultado que se almacenará en un fichero clasificado por el sensor así como por la determinación de la validez de la comparación.

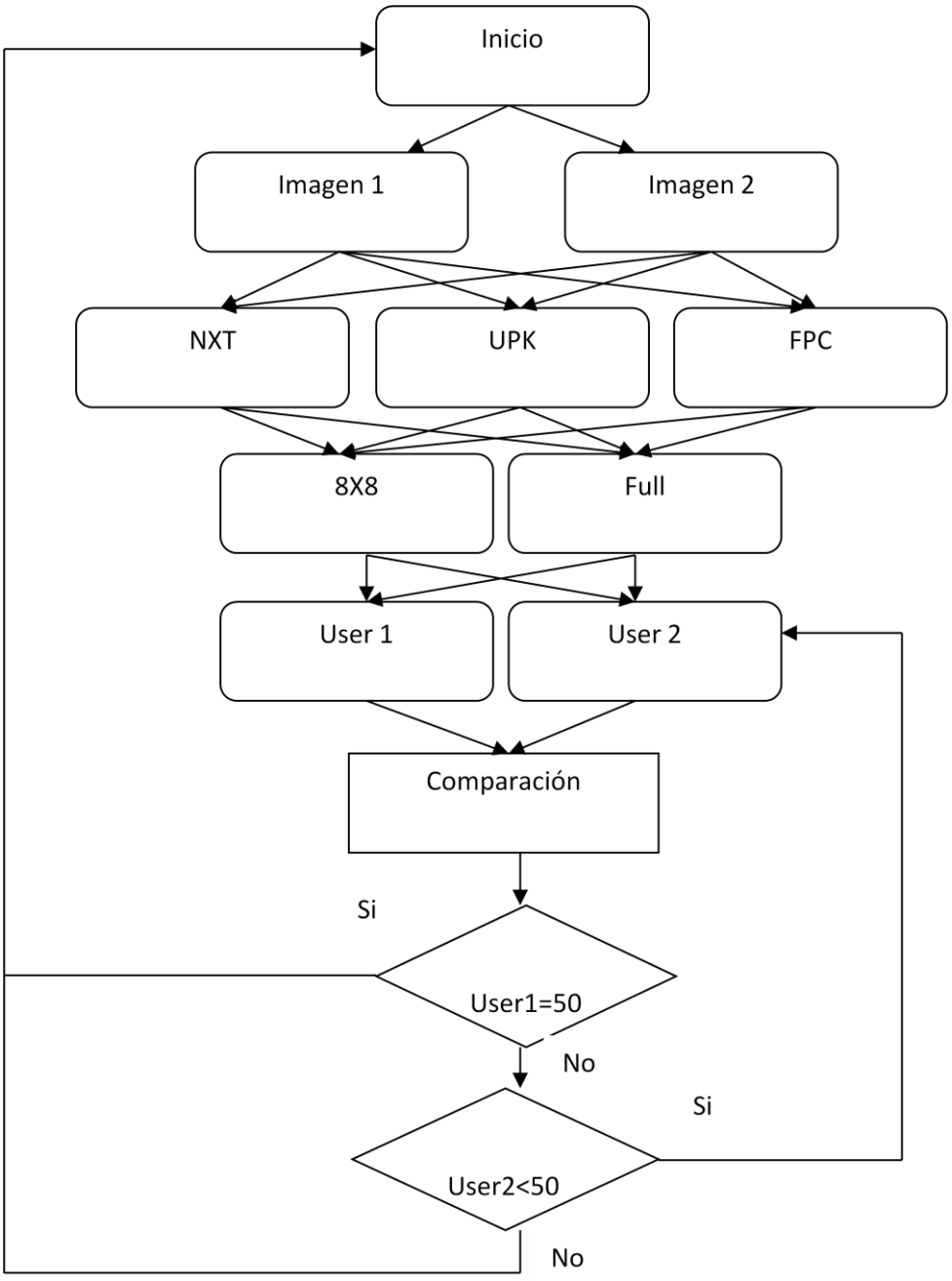

Figura 24. Diagrama lógico de la app de procesado

3.3.2. Aplicación del cálculo de rendimiento

La aplicación del cálculo de rendimiento se implementa a partir de la herramienta BioSecure Tool desarrollada en el punto 3.2.4 del presente documento.

Esta herramienta es la encargada de proporcionar diversos factores estadísticos así como de la creación de tres tipos de gráficos (ROC, DET y FAR vs FRR). Para ello llamaba a la función EER_DET_conf que era la encargada de llamar al resto de funciones de la herramienta para la obtención de los valores, como se explica en el punto 3.3.2.1. Esta aplicación está ya implementada por lo que no ha sido necesario modificar ninguno de sus parámetros en lo que a programación se refiere. Como valores de entrada se encuentran los ficheros genuinos e impostores y como valor de salida el valor de OP y el EER. Su composición se muestra en la figura 28.

Ha sido muy útil en el desarrollo del estudio por su aportación de valores exactos y visuales para cualquier usuario.

3.3.2.1. Función EER_DET_conf

Esta función es la encargada de llamar al resto de funciones con el fin de obtener todos los resultados que nos proporciona esta herramienta. La EER_DET_conf se desarrolla en el entorno MatLab y cuenta con unos parámetros de entrada que se introducen en la función.

$$[EER] = EER\ DET\ conf(clients, imposteurs, OPvalue, pas0)$$

Siendo:

- Clients: resultados obtenidos de la comparación en el caso en el que estos sean genuinos.
- Imposteurs: resultados obtenidos de la comparación en el caso en el que estos sea impostores.
- OPvalue: valor porcentual que determina el nivel de seguridad del sistema.
- Pas0: resolución de las gráficas de salida.

3.3.2.2. Gráfica de resultados ROC

Como ya se introdujo en el apartado 3.2.4., una curva ROC, es aquella que se encarga de representar gráficamente la sensibilidad frente a (1- especificación) para un sistema binario al variar el umbral de discriminación. También se puede entender como la razón o ratio de verdaderos positivos frente a la razón o ratio de falsos positivos, según varíe el umbral de discriminación que delimita el valor para el cual se asegura que un caso es positivo [30]. Esta curva en el estudio de las comparaciones nos facilitará conocer el modelo más óptimo para los diferentes casos presentados::

- Full vs Full
- 8x8 vs 8x8
- Full vs 8x8

Algunos parámetros a tener en cuenta en las curvas ROC son:

- Punto de inserción de la curva ROC con la línea convexa a la línea de discriminación.
- El área entre la curva ROC y la línea convexa a la línea de discriminación.
- El área bajo la curva ROC.

En nuestro caso, se representa en el eje de abscisas la tasa FMR o FAR, mientras que en el eje de ordenadas se representa la diferencia (1-Tasa FNMR) o (1-FRR). Comúnmente se emplea la escala logarítmica para poder representar mejor las curvas. Para determinar la calidad de dicha curva se observará su linealidad. Para el estudio de la calidad de esta curva se tendrá en cuenta que un buen sistema tendrá una curva muy próxima al valor máximo situado a la izquierda de la gráfica. Así puede observarse gráficamente en la figura 25.

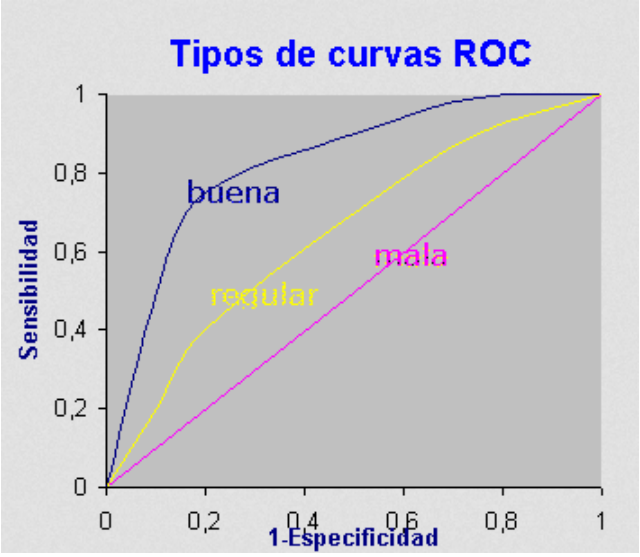

Figura 25. Tipos de curva ROC y su clasificación [31]

El objetivo final de estas curvas es conseguir demostrar la precisión y calidad de los sistemas a comparar. A continuación, en la figura 26, se delimitan las áreas que deben ser estudiadas para evaluar a una gráfica ROC.

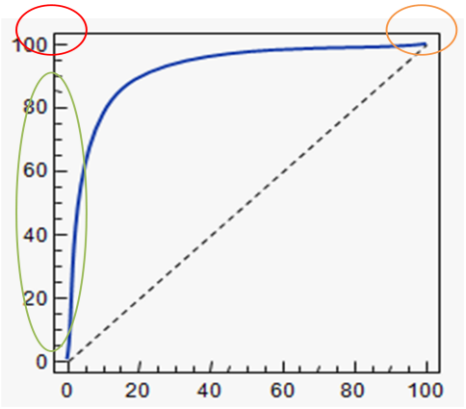

Figura 26.Características curvas ROC [32]

En dicho punto el porcentaje de verificación es máximo y por tanto la falsa aceptación es de 0.

En el área comprendida más cercana a la parte izquierda de la gráfica, el sistema indica seguridad. En estos puntos la FMR es baja y por lo tanto el sistema tiende en mayor medida a rechazar usuarios legítimos que en aceptar impostores.

La esquina superior derecha indica el máximo grado de aceptación a cualquier usuario. Es decir, el porcentaje de verificación es del 100%. De forma general, estos puntos pueden ser considerados convenientes para que los usuarios genuinos no sean rechazados falsamente.

3.3.2.3. Gráfica de resultados DET

La curva DET o Detection error Tradeoff, se trata de un esquema gráfico para sistemas de clasificación binaria, en el cual se enfrentan los resultados de falso rechazo frente a la falsa aceptación.

Los ejes x e y son escalados de manera lineal por sus desviaciones normales estándar. Al igual que en la curva ROC esta curva es muy utilizada para documentar los resultados de la evaluación de rendimiento. Solo pueden calcularse si el sistema devuelve valores de similitud. Cada punto de la gráfica, por tanto, representará los valores de ambas tasas para los diferentes márgenes de decisión [33]. En este tipo de curvas el eje de abscisas contará con la representación de la tasa FMR o FAR, mientras que el eje de ordenadas se representa la tasa FNMR o FRR, tal y como se representa en la figura27.

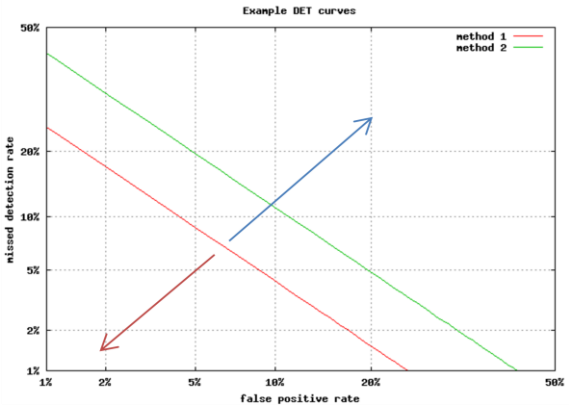

Figura 27.Tendencia en curvas DET [33]

Una tendencia hacia la esquina superior derecha delimita una peor calidad de los resultados llevados a evaluación

Conforme disminuye la gráfica tanto en el eje x como en el eje y ,tendencia hacia la esquina inferior izquierda, aumentará la calidad de la evaluación.

3.3.2.4. Diseño lógico de la aplicación del cálculo de rendimiento

A continuación se describe en la figura 28, la lógica seguida por la aplicación estadística.

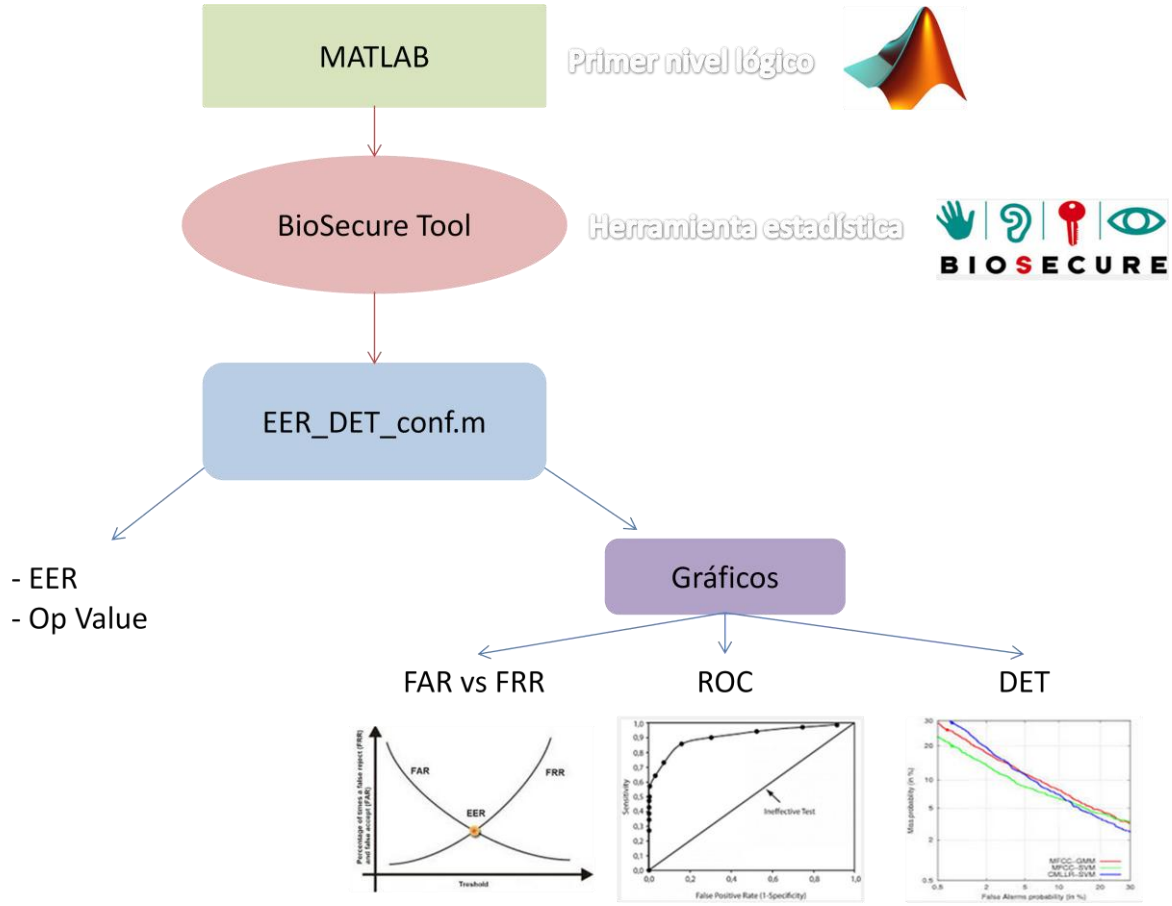

Figura 28. Diagrama lógico app estadística

4. DESARROLLO

En este capítulo se tratan los desarrollos de cada una de las aplicaciones utilizadas en el estudio. En dichos desarrollos se tratan las ideas iniciales, los problemas que han surgido durante su realización y los resultados finales obtenidos.

4.1. Desarrollo de la aplicación de procesado

Una vez terminada con la evaluación, el objetivo del trabajo es el de conocer la influencia del tamaño de la muestra en el rendimiento de un sistema biométrico basado en huella dactilar. Para la obtención de huellas de menor tamaño ha sido necesario recortar las almacenadas en la base de datos. Con las muestras a tamaño real y las recortadas se evaluará el comportamiento de cada uno de los sensores para cada tamaño de imagen.

A continuación, se explica cómo ha evolucionado la aplicación de procesado hasta conseguir la versión definitiva.

4.1.1. Versión código 01

La primera versión o "*V01"* se encargaba de seleccionarlas imágenes elegidas por el usuario. Para ello el programa solicitaba que se tomase una imagen de huella de la BBDD, imagen 1 o muestra a comparar. A continuación, una vez seleccionada esta primera imagen, se requería la inserción de la segunda. El objetivo inicial era el de mostrar por pantalla la cantidad de minucias de cada muestra y posteriormente, compararlas para obtener un resultado. Supuso un primer contacto con el código implementado y con el algoritmo.
Para comenzar con el desarrollo de la aplicación y comprobar su correcta ejecución, se contaba con las muestras de 2 usuarios para realizar las comparaciones. Entonces, comparar de manera manual cada una de las imágenes, a pesar de ser un arduo trabajo, era posible.
Sin embargo, al conocer el tamaño real de la base de datos, y la gran cantidad de muestras que contenía, se rediseño por completo la aplicación con el fin de que esta fuese automática.

4.1.2. Versión código 02

La segunda versión surgió para solventar el problema de la selección manual de las imágenes. En ella se realiza una remodelación de código que perseguía dos objetivos:

- El objetivo principal era el de automatizar el proceso de selección de imágenes.

- Por otro lado, a partir de la automatización nace el interés por reducir tiempos los tiempos de procesado de comparación.

La remodelación comenzó con una disminución de código y con la creación de operaciones más simples que ayudasen al programa a ser más rápido y eficiente. A pesar de conseguir remodelarlo y ser más eficiente, aún el sistema no era automático.

4.1.3. Versión código 03

En la V03, se estudió la distribución de la base de datos inicial, previa a la BBDD-TFG-Cropped. Esta se componía de una carpeta sensor, dentro de la cual se encontraban los diferentes usuarios y donde se albergaban todas las imágenes de las muestras, tanto los reclutamientos como las verificaciones. Teniendo en cuenta esto se organizó la estructura de programación correspondiente a la Figura 29.

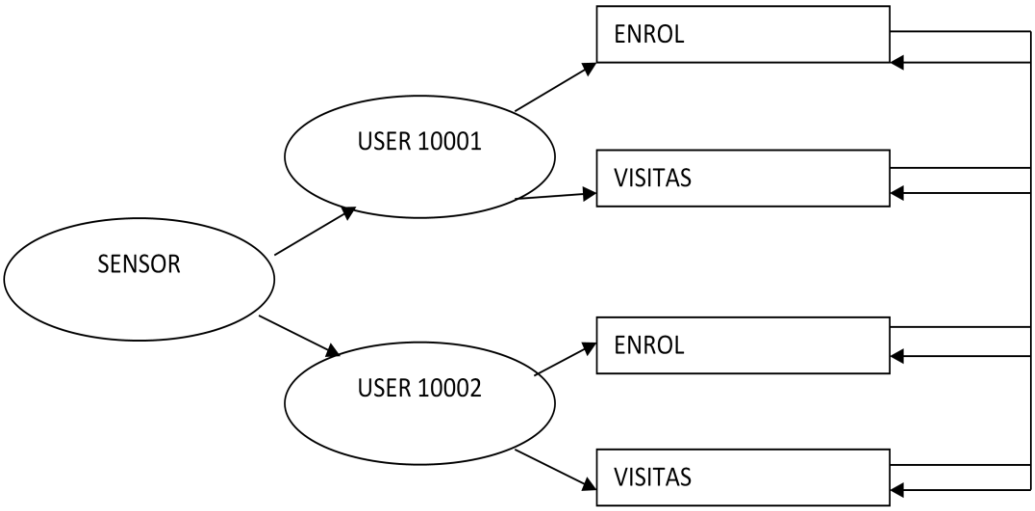

Figura 29.Lógica de programación VO. cód. 3

La comparación se desarrollaría tal y como se muestra en la figura 29. Es decir, comparar todas las imágenes tanto de reclutamiento como de verificación, de manera uno a todos (1:N). Por ello, apareció el problema de la ingente cantidad de muestras a comparar.

4.1.4. Versión código 04

Con dicho problema de tamaño, surgió la necesidad de crear una V04. En esta versión se comenzaron a establecer las bases de una correcta implementación que permitiese una alta optimización del código. Comenzó con el cambio de código de aplicación de consola de Visual Studio, a una interfaz de programación en *Windows Presentation Foundation (WPF)*.

La presentación WPF ofrecía la oportunidad de crear una interfaz más visual para el usuario, pretendiendo además mejorar la accesibilidad en las opciones de comparación, a través de la generación de diferentes botones de selección y actuación. Además se implementó una pequeña función que se encargaba de tomar una imagen de la base de datos, copiarla y cortarla dependiendo del tamaño definido, ya sea 8x8 o imagen completa.

El proceso de comparación para entonces era el siguiente. El usuario seleccionaba el sensor, posteriormente el tamaño de la imagen 1 y a continuación el tamaño de la imagen 2, tras clickear el botón *compare* la aplicación se ejecuta. El funcionamiento del programa se componía de varias instrucciones *if´s,* encargadas de acceder a cada uno de los códigos dependiendo de la selección del usuario. En cada *if* se localizaba un código específico, que mediante el uso de bucles *for* hacía que el programa recorriese la dirección o *path*. Una vez

recorridos todos los bucles *for,* el programa obtenía la dirección completa de acceso a la primera y segunda imagen. A continuación el código llamaba a la función de detección de minucias proporcionada por el algoritmo NBIS.

Este algoritmo se encarga de extraer todas las minucias tanto de la imagen 1 como de la imagen 2 y compararlas. Una vez terminada dicha comparación se obtenía el valor de la comparación por pantalla. Tras conseguir los objetivos establecidos en la versión tres, aparecía el problema del almacenamiento de los resultados

4.1.5. Versión código 05

La versión 5 se crea con el fin de generar un método que permita almacenar todos los resultados. Una vez obtenida la información relativa a la comparación, el programa crea un fichero global para todos los resultados de las comparaciones y se cierra tras la finalización de éste. Pero de nuevo el sentido del estudio tomaba otro camino, esto se debe a:

- La necesidad de conocer la BBDD TFG Cropped para poder programar el acceso a las diferentes carpetas donde se organizaban las imágenes

- La necesidad de una lógica del programa, para realizar la comparación 1:N.

- La disminución del tiempo de procesado, crucial para una evaluación más rápida y eficiente.

- La necesidad de organizar los ficheros para cada una de las pruebas y para cada uno de los resultados de una misma prueba, donde se puedan encontrar los datos.

4.1.6. Versión código 06

Tras estudiar los puntos mencionados anteriormente se crea una versión 6 con un carácter aparentemente más definitivo, que trataba de resolver los problemas de la siguiente manera:

- La BBDD TFG Cropped fue proporcionada por el departamento con uso exclusivo en laboratorio. Dicha base de datos ya contaba con una organización definitiva tal y como se redactaba en el punto 2.6.4 del presente documento.

- Se observó y estudió dicha base de datos comprendiendo como reprogramar el código para el acceso. A su vez las imágenes ya estaban cortadas por lo que la función para el corte de las imágenes no era necesaria.

- Por otro lado la lógica del programa cambió. El objetivo del estudio no era el de comparar todas las muestras con ellas mismas y con el resto, sino que era necesario diferenciar entre reclutamiento y verificación. El objetivo era el de comparar los

datos de las muestras reclutadas con aquellas muestras que fuesen verificaciones, tal y como se observa en la figura 30.

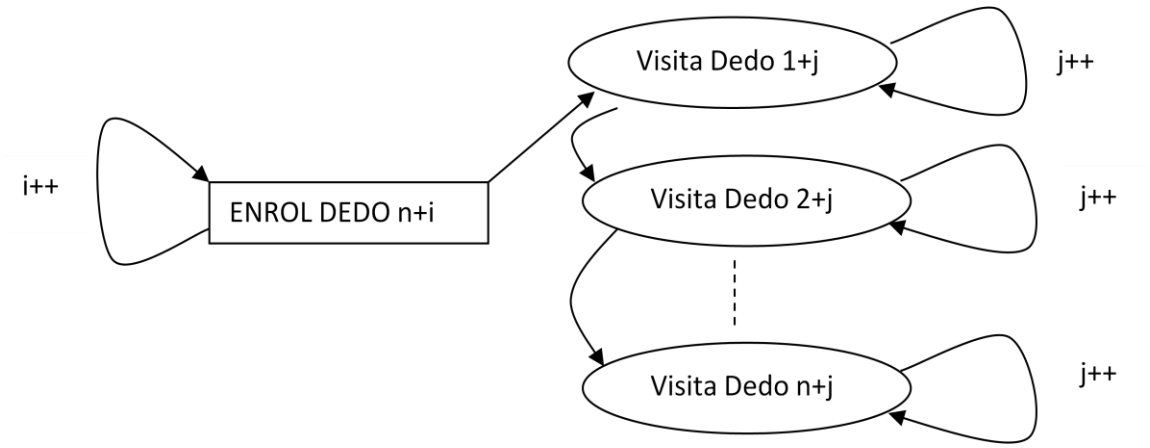

Figura 30.Lógica de programación VO.cod 6

En la figura 30, aún no se podía especificar la cantidad de reclutamientos que había por dedo en cada usuario "*i*", ni tampoco la cantidad de verificaciones *"j"*.

- Se continuó con el proceso de mejora y progreso del código.

- Para poder organizar los ficheros y por tanto los datos obtenidos se procedió a dar diferentes nombres de fichero dependiendo de los datos de usuario de *enrol* y muestra de visita a comparar. Es decir, se creaba un fichero cuyo nombre era usuario 1, nombre del sensor y dentro contenía todas las comparaciones de un mismo usuario, con todas las posibles verificaciones de todos los usuarios.

Sin embargo, aún era necesario el estudio de numerosos factores como los que se presentan a continuación:

- El objetivo no era comparar todos los reclutamientos de un dedo con todas las visitas, se tenía que tener en cuenta sólo la mejor muestra perteneciente a un usuario para la comparación. Para ello se centró el estudio en el factor NFIQ, por ello, se creó un *vector* de 6 posiciones cuya funcionalidad se explica en la figura 31.

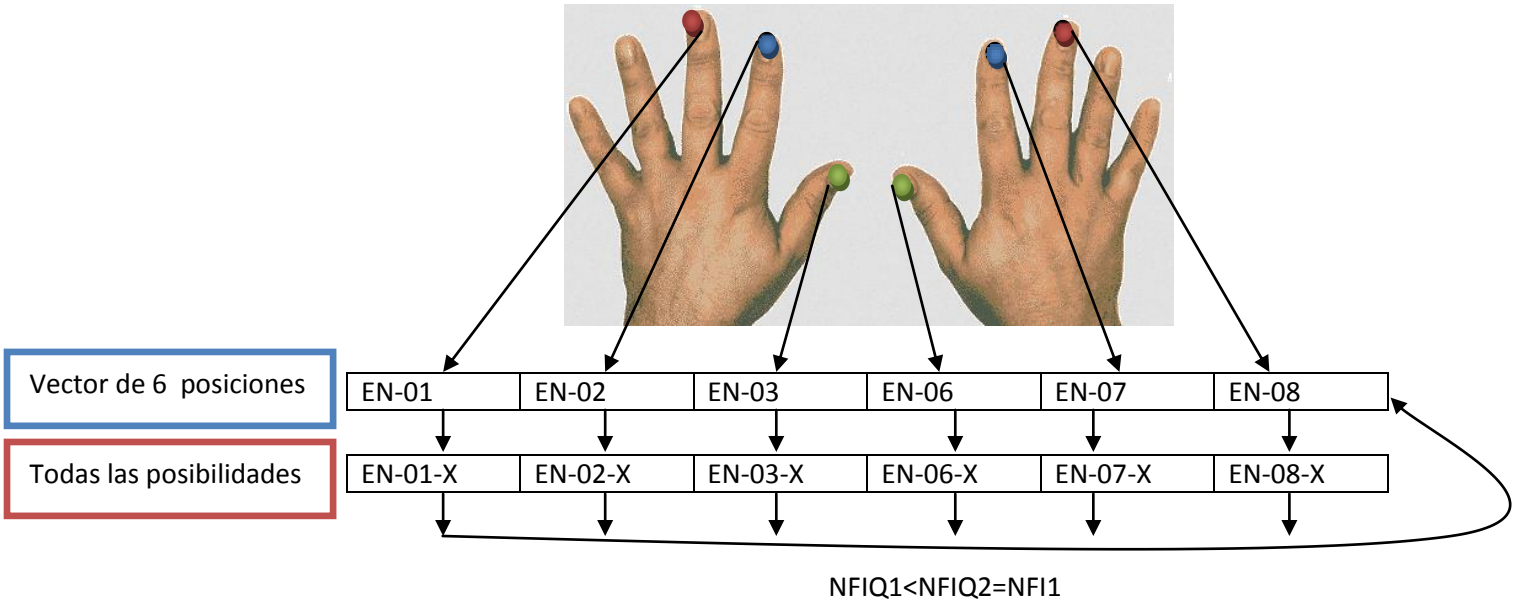

Figura 31.Lógica de programación VO final

- Se generó una comparación dependiendo del nombre de la ruta o *path* para el acceso a cada imagen. Es decir, si se está rellenando la posición 1 del vector, tendrá en cuenta todos los archivos con EN-01 en su ruta, los recorrerá y situará aquel cuyo NFIQ sea menor. Para ello, reemplazará la ruta por una nueva. Esta acción se repite para las 6 posiciones. Por otro lado todos aquellos reclutamientos con un factor de calidad NFIQ igual a 5, no eran muestras aceptables. Por ello, no se incluían en el estudio. Se vetó el acceso, a imágenes con NFIQ igual a 5, a través de una función *if* .

- Otro problema añadido eran los casos en los que un dedo solo tuviese reclutamientos NFIQ igual a 5, el programa no rellenaba esa posición y provocaba la aparición de una excepción referente a los datos de entrada, donde se explicaba que no se localizaba la imagen a comparar.

4.1.7. Versión de código final

Finalmente, apareció la versión 7 que se generó con un carácter definitivo. En ésta el código corregía todos los errores previamente mencionados y ofrecía:

- Implementación de un código global, para todas las pruebas, a modo de función cuyos parámetros de acceso venían determinados por un *switch* de posibilidades.
- Automatización del proceso con el vector de rutas de reclutamientos de 6 posiciones y la eliminación de todas aquellas imágenes NFIQ 5.
- En caso de aparecer un dedo con tan sólo pruebas NFIQ 5, el programa directamente lo saltaba y continuaba con el siguiente dedo o usuario.
- Generación de dos ficheros genuino, en caso de coincidencia de la ruta, e impostor, en caso de no conocimiento de la ruta.

4.2. Desarrollo de la aplicación para el cálculo del rendimiento

Como se ha especificado en el punto 3.3.2 del presente escrito, para la obtención de los resultados estadísticos es necesaria la aplicación BioSecure Tool. El desarrollo de esta aplicación ha sido ínfimo debido a que desde el inicio viene predefinida para la obtención de resultados. Una vez haya finalizado la generación de resultados por parte de la aplicación de comparación, éstos estarán organizados en ficheros de resultados genuinos e impostores. El primer paso es importar estos resultados de manera que comprendan un vector de resultados, tal y como se muestra en la Figura 32.

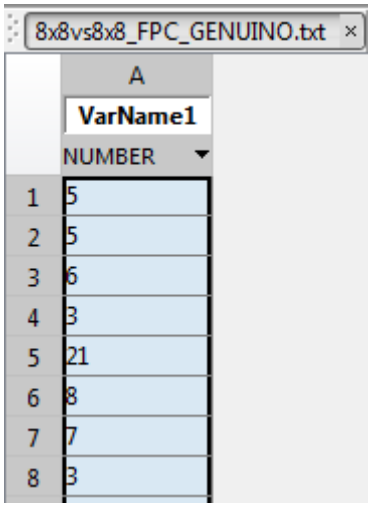

Figura 32. Inserción de datos

Una vez estos resultados sean importados, se introducirán en la función estadística EER_DET_conf explicada en el punto 3.3.2.1. Obteniéndose así los resultados estadísticos

```
>> [EER confInterEER OP confInterOP]=EER_DET_conf(nxt8v8gen,nxt8v8imp,100,10000)
```

5. RESULTADOS

A continuación se presentan los tres análisis propuestos para conocer el rendimiento del sistema biométrico dependiendo del tamaño de la muestra. Se iniciará con la evaluación del NFIQ de las muestras, seguidamente se realiza un análisis del tiempo de procesado y por último una evaluación gráfica de cada una de las posibles opciones.

5.1. Estudio de calidad de las muestras

A continuación se presenta el estudio de calidad de las muestras contenidas en la Base de datos de huellas dactilares mediante el parámetro NFIQ. El parámetro NFIQ explica la calidad de una huella dactilar, siendo 5 el valor más bajo y 1 el más alto.

5.1.1. Muestras FPC

A continuación, en la fgura33 y en la tabla 2 se muestran la cantidad de imágenes, tanto de reclutamiento como de verificación, presentes en el sensor FPC clasificadas por la calidad de la imagen. El valor de calidad predominante es el 3, tanto para imágenes completas como para las 8x8. El número de muestras a comparar es elevado, tal y como muestra la tabla2 se analizarán 3550 imágenes de tamaño reducido y 9295 de tamaño completo.

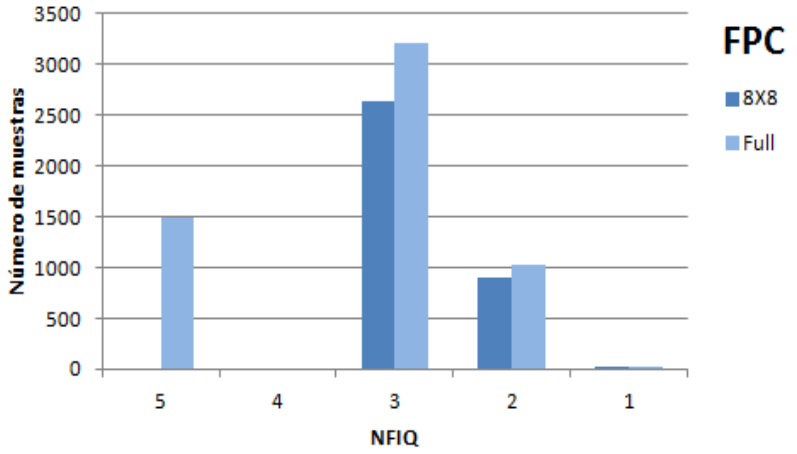

Figura 33. Histograma FPC

NFIQ	8X8	Full
5	0	1491
4	0	0
3	2631	3203
2	894	1025
1	25	26

Tabla 2.Enumeración de muestras FPC

5.1.2. Muestras NXT

A continuación, en la fgura34 y en la tabla 3 se muestran la cantidad de imágenes, tanto de reclutamiento como de verificación, presentes en el sensor NXT clasificadas por su calidad. El factor de calidad predominante es el 2.Ésto implica que la calidad de la captación es muy buena.

El número de muestras a comparar es alto, tal y como muestra la tabla3 se analizarán 4274 imágenes de tamaño reducido y 5016 de tamaño completo. En comparación con el sensor FPC, los resultados del NXT demuestran que la calidad de captación del sensor térmico es mucho mayor que la del capacitivo. Además, el número de imágenes a estudiar disminuye.

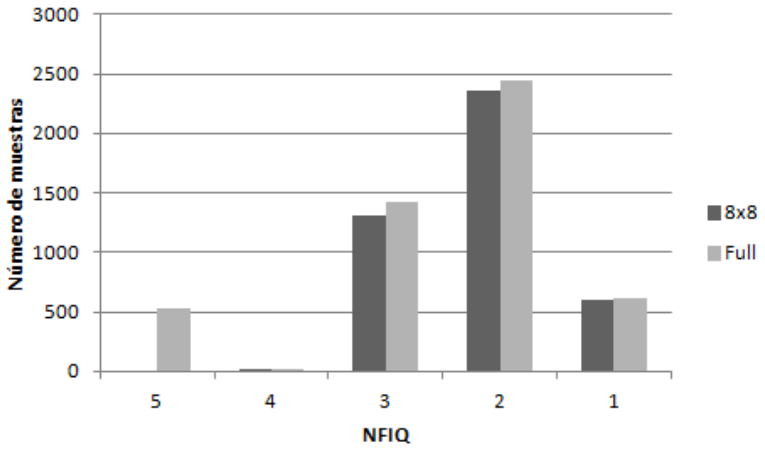

Figura 34.Histograma NXT

NFIQ	8X8	Full
5		530
4	1	1
3	1307	1422
2	2361	2442
1	605	621

Tabla 3.Enumeración de muestras NXT

5.1.3. Muestra UPK

A continuación, en la fgura34 y en la tabla 4 se muestran la cantidad de imágenes, tanto de reclutamiento como de verificación, presentes en el sensor UPK clasificadas por su calidad. En este caso, al contrario que en los anteriores, cuenta con una diferencia muy grande de imágenes de tamaño completo en comparación a las de tamaño reducido. La ingente cantidad de muestras de tamaño completo indica que la captación de huellas por parte del sensor no es positiva, es decir, necesita captar numerosas muestras para finalizar la evaluación. El factor de calidad que cuenta con más muestras es el 3. Además, se analizarán 3654 imágenes de tamaño reducido y 63535 de tamaño completo.

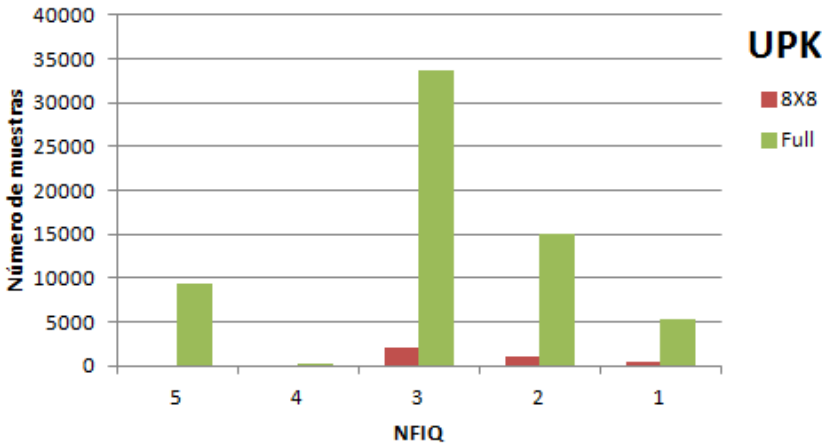

Figura 35.Histograma UPK

NFIQ	8X8	Full
5		9344
4		4
3	2182	33695
2	1025	15076
1	447	5416

Tabla 4.Enumeración de muestras UPK

5.2. Estudio del Tiempo de procesado

Con el fin de comprobar la calidad de procesamiento del código, se ha procedido a cronometrar el tiempo de procesado para cada una de las pruebas realizadas.

5.2.1. FPC 8x8 Vs 8x8

Para la realización del análisis de tiempo se han tomado dos imágenes aleatorias. En la figura 36, izquierda, se localiza el tiempo que tarda el programa en completar un solo análisis. Mientras que la figura 36, derecha, muestra el tiempo que tarda en procesar todas las comparaciones de un *Enrol* con todas las visitas

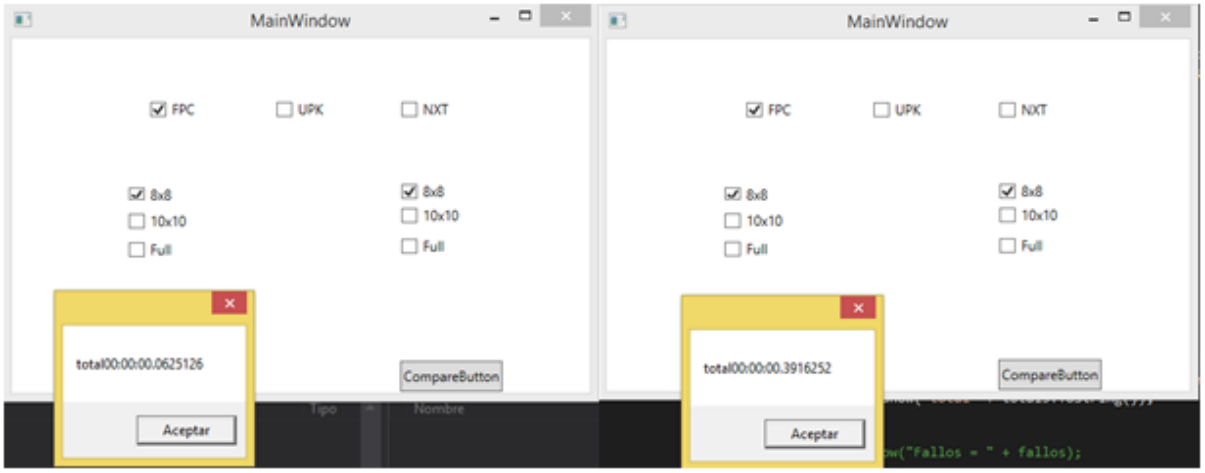

Figura 36.Resultado de tiempos de comparación individual y total 8x8 vs 8x8 FPC

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.062551 segundos
Tiempo de comparación 1vs*	00.3916252 segundos

Tabla 5.Tiempo de comparación 8x8 vs 8x8 FPC

Como se puede observar, y a pesar de ser el primer análisis generado, el tiempo de procesamiento no es excesivamente alto para una comparación y es bastante aceptable para un número inferior a 50. Sin embargo el número de comparaciones de cada análisis es muy grande por lo que el tiempo necesario es demasiado elevado:

$$0{,}39\frac{s}{enrol * user} * 50\ user = 19{,}5\frac{s}{enrol}$$

$$19{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50 user = 5850\ segundos$$

5.2.2. FPC Full Vs 8x8

A continuación se presenta el tiempo de comparación individual y total representado en la figura 37.

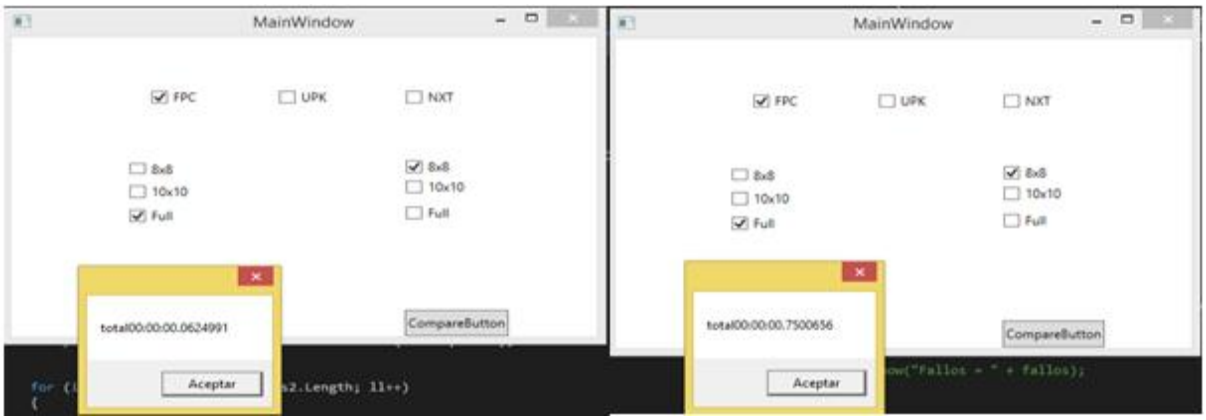

Figura 37.Resultado de tiempos de comparación y totales Full vs 8x8 FPC

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.0624991 segundos
Tiempo de comparación 1vs*	00.7500065 segundos

Tabla 6.Tiempo de comparación Full vs 8x8 FPC

Aproximadamente se mantiene el tiempo de comparación general ya que el número de *Enrol* y visitas serán los siguientes:

$$0{,}75\frac{s}{enrol * user} * 50\ user = 37{,}5\frac{s}{enrol}$$

$$37{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50 user = 11250\ segundos$$

5.2.3. FPC Full Vs Full

A continuación se localiza el tiempo de procesado de dos imágenes *a tamaño completo* para la muestra de reclutamiento y verificación, (figura38 izquierda), y de un reclutamiento con todas las visitas de un usuario (figura38 derecha).

En este caso al aumentar la cantidad de comparaciones aumenta el tiempo de procesado de la imagen:

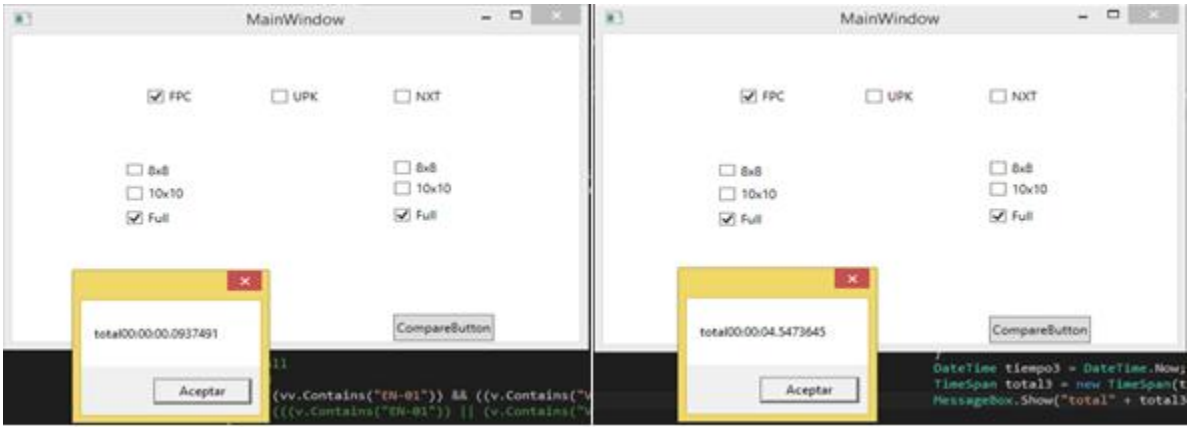

Figura 38.Resultado de tiempos de comparación y totales Full vs Full FPC

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.04547364 segundos
Tiempo de comparación 1vs*	00.093749 segundos

Tabla 7.Tiempo de comparación Full vs Full FPC

$$0{,}09\frac{s}{enrol * user} * 50\ user = 19{,}5\frac{s}{enrol}$$

$$19{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50 user = 5850\ segundos$$

5.2.4. NXT 8x8 Vs 8x8

En el caso de la utilización de la tecnología térmica con imágenes de tamaño 8x8, se obtienen los tiempos de procesado localizados en la figura39.

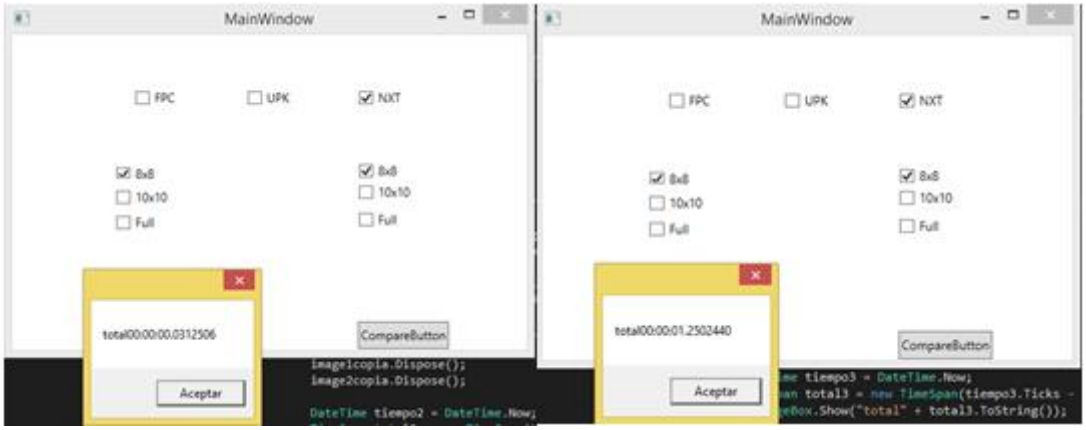

Figura 39. Resultado de tiempos de comparación y totales 8x8 vs 8x8 NXT

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.0312506 segundos
Tiempo de comparación 1vs*	01.2502440 segundos

Tabla 8.Tiempo de comparación 8x8 vs 8x8 NXT

$$1{,}25\frac{s}{enrol * user} * 50\ user = 62{,}5\frac{s}{enrol}$$

$$62{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50 user = 18750\ segundos$$

5.2.5. NXT Full Vs 8x8

En el caso de utilización de la tecnología térmica con imágenes de tamaño 8x8 frente a imágenes de tamaño completo, se obtienen los tiempos de procesado localizados en la figura 40 y en la tabla 9.

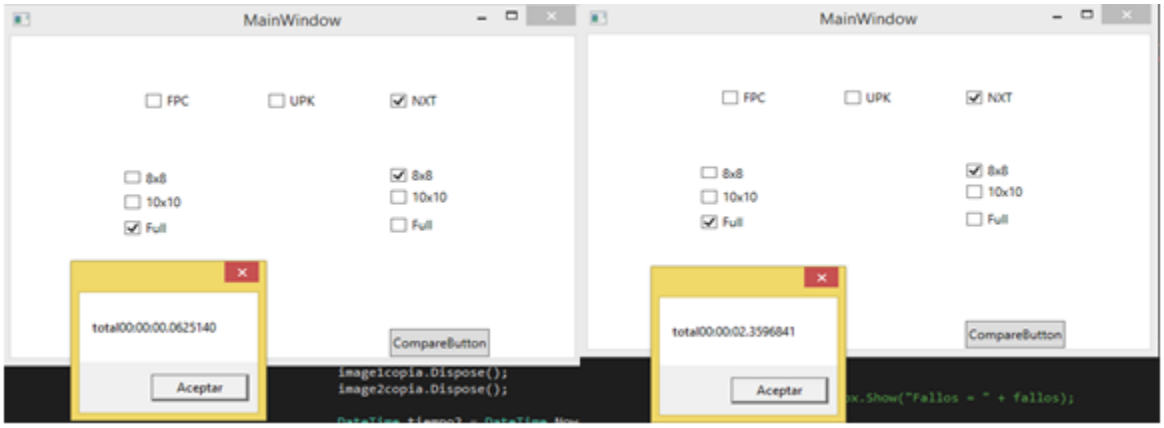

Figura 40.Resultado de tiempos de comparación y totales Full vs 8x8 NXT

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.0312506 segundos
Tiempo de comparación 1vs*	01.2502440 segundos

Tabla 9.Tiempo de comparación Full vs 8x8 NXT

$$1{,}25\frac{s}{enrol * user} * 50\ user = 62{,}5\frac{s}{enrol}$$

$$62{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50user = 18750\ segundos$$

5.2.6. NXT Full Vs Full

En el caso de utilización de la tecnología térmica con imágenes de tamaño completo, se obtienen los tiempos de procesado localizados en la figura41 y en la tabla 10.

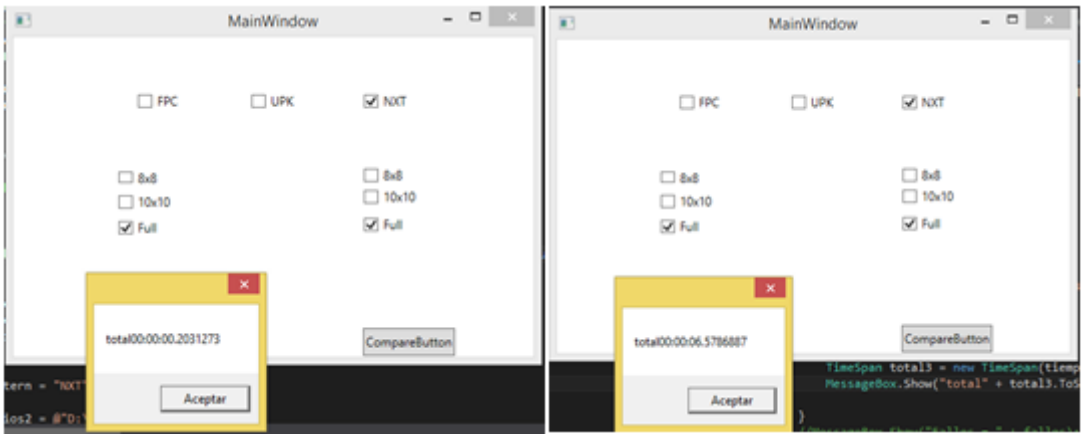

Figura 41. Resultado de tiempos de comparación y totales Full vs Full NXT

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.2031273 segundos
Tiempo de comparación 1vs*	06.5718688 segundos

Tabla 10.Tiempo de comparación Full vs Full NXT

$$6{,}57\frac{s}{enrol * user} * 50\ user = 328{,}5\frac{s}{enrol}$$

$$328{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50user = 98550\ segundos$$

5.2.7. UPK 8x8 Vs 8x8

En el caso de utilización de la tecnología capacitiva con el sensor UPK con imágenes de tamaño 8x8, se obtienen los tiempos de procesado localizados en la figura42 y en la tabla 11.

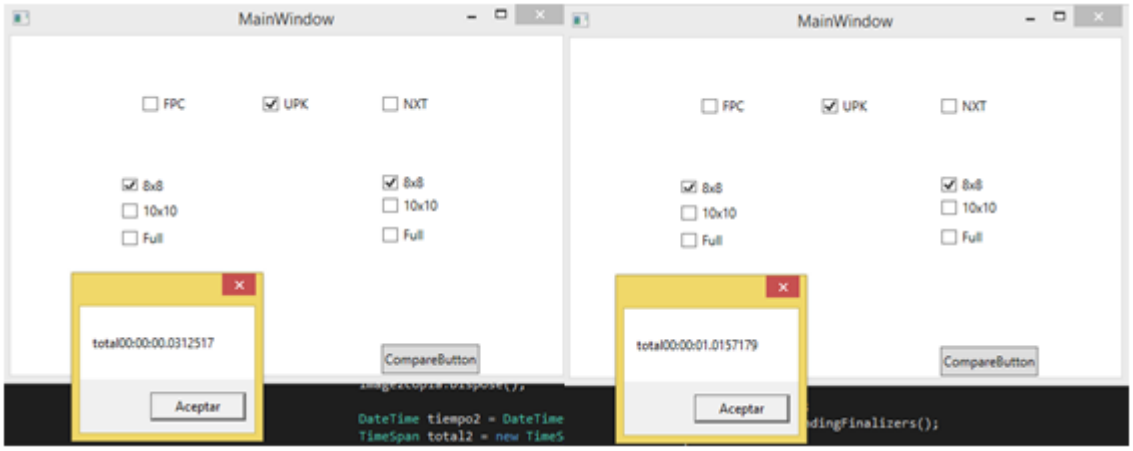

Figura 42. Resultado de tiempos de comparación y totales 8X8 vs 8X8 UPK

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.0312517 segundos
Tiempo de comparación 1vs*	01.0157179 segundos

Tabla 11.Tiempo de comparación 8x8 vs 8x8 UPK

$$1{,}01\frac{s}{enrol * user} * 50\ user = 50{,}5\frac{s}{enrol}$$

$$50{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50user = 15150\ segundos$$

5.2.8. UPK Full Vs 8x8

En el caso de utilización de la tecnología capacitiva con el sensor UPK con imágenes de tamaño 8x8 y *"FullSize"*, se consiguen los tiempos de procesado localizados en la figura43 y en la tabla 12.

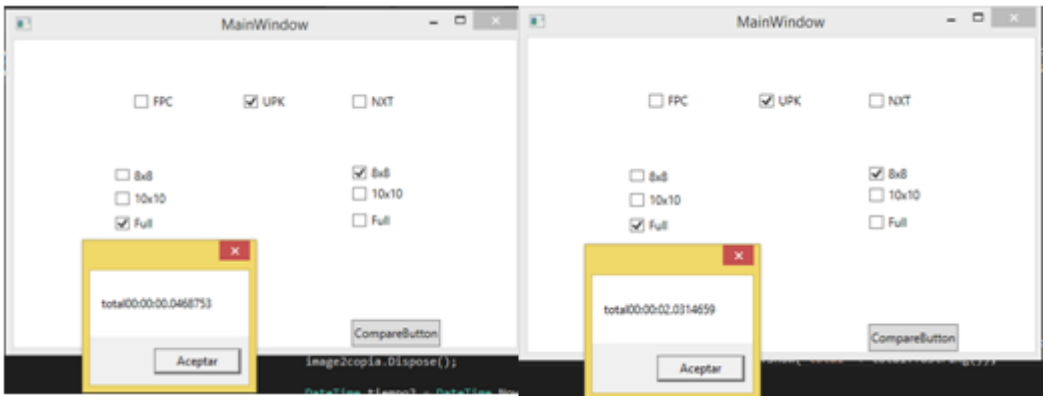

Figura 43. Resultado de tiempos de comparación y totales Full vs 8X8 UPK

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.0468753 segundos
Tiempo de comparación 1vs*	02.0311465 segundos

Tabla 12.Tiempo de comparación Full vs 8x8 UPK

$$2{,}03\frac{s}{enrol * user} * 50\ user = 101{,}5\frac{s}{enrol}$$

$$101{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50 user = 30450\ segundos$$

5.2.9. UPK Full Vs Full

En el caso de utilización de la tecnología capacitiva con el sensor UPK con imágenes de tamaño "*FullSize*", se consiguen los tiempos de procesado localizados en la figura 44 y en la tabla 13.

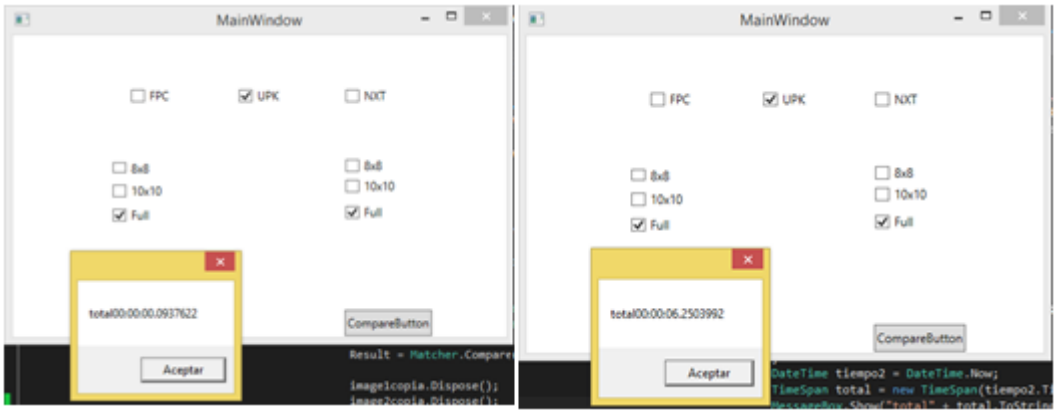

Figura 44. Resultado de tiempos de comparación y totales Full vs Full UPK

Tabla de Tiempos	
Tiempo de comparación 1vs1	00.0937622 segundos
Tiempo de comparación 1vs*	06.2503992 segundos

Tabla 13.Tiempo de comparación Full vs Full UPK

$$6{,}25\frac{s}{enrol * user} * 50\ user = 312{,}5\frac{s}{enrol}$$

$$312{,}5\frac{s}{enrol} * 6\frac{enrol}{user} * 50 user = 93750 segundos$$

5.3. Full vs Full

A continuación se presentan los principales resultados obtenidos en las curvas Full vs Full de todos los sensores y muestras a evaluar.

5.3.1. FAR vs FRR

Las figura 45, 46 y 47, muestran las curvas FAR vs FRR para imágenes Full vs Full. De la gráfica podemos obtener el valor EER, explicado anteriormente en el punto 2.1.5. A medida que disminuye el valor del EER, mejor será el sistema. En esta primera parte se estudian los sistemas de imágenes completas, por lo que el porcentaje de igual error se mantiene en valores bajos de aproximadamente 14. En el análisis de la curva FAR vs FRR, el algoritmo estadístico ha determinado que el mejor sistema es el UPK full vs full, el cual obtiene un valor de EER de 13.2120, localizado en la figura 47 y en la tabla 16.

A continuación, se presenta la curva FAR vs FRR correspondiente al sensor FPC.

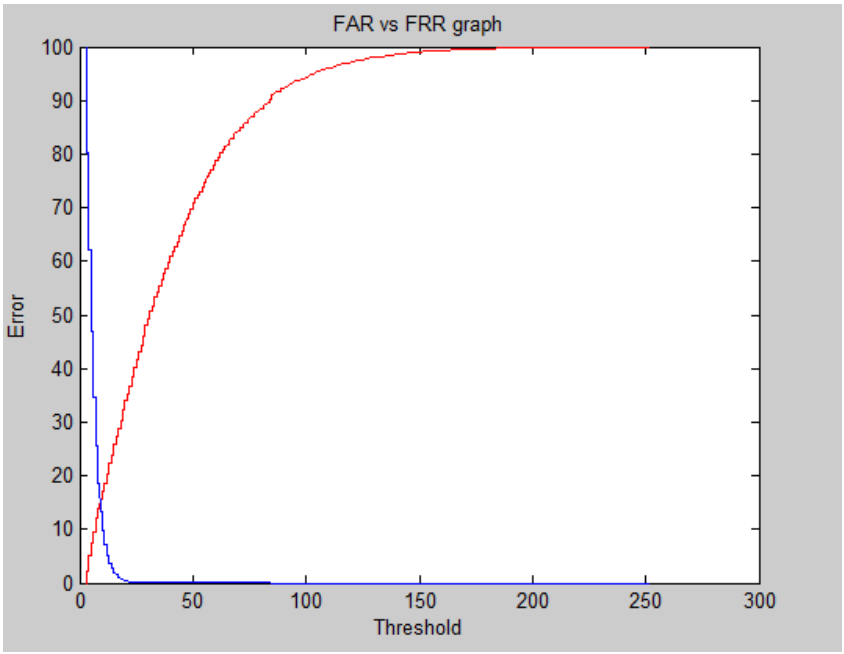

Figura 45. FAR vs FRR FPC full vs full

Donde se logran los siguientes valores estadísticos

EER	14,5094
ConfInterEER	0,4818

Tabla 14. Resultados estadísticos FAR vs FRR FPC

Para continuar con el análisis se expone en la figura 46 la curva FAR vs FRR del sensor NXT

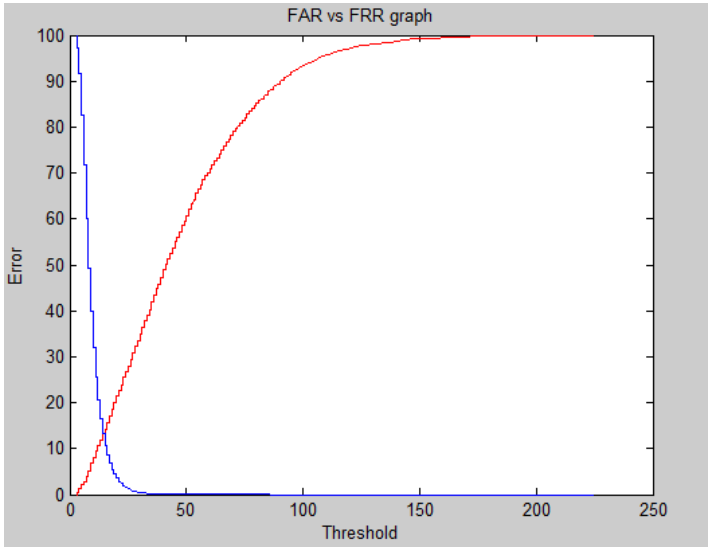

Figura 46. FAR vs FRR NXT full vs full

Donde se exponen los siguientes valores estadísticos

EER	13.6120
ConfInterEER	0.4468

Tabla 15. Resultados estadísticos NXT full vs full

Para finalizar se localiza en la figura 47 de la curva FAR vs FRR del sensor UPK

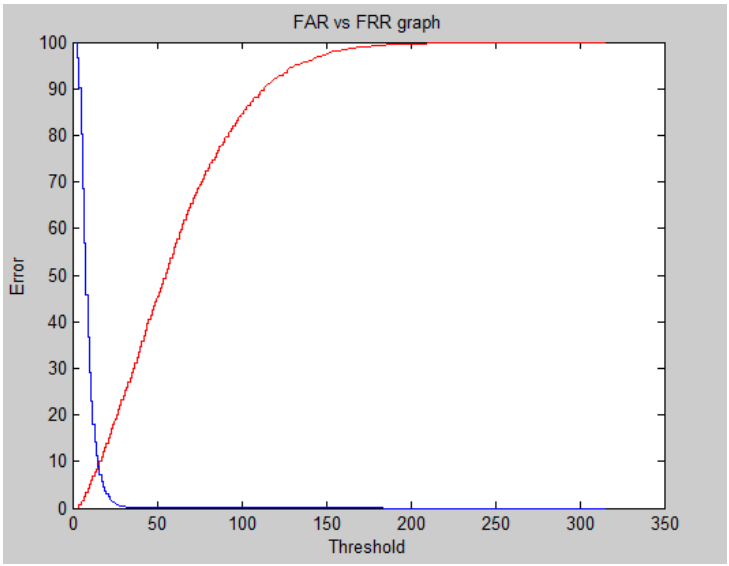

Figura 47. FAR vs FRR UPK full vs full

Donde se consiguen los siguientes valores estadísticos

EER	13.2120
ConfInterEER	0.4468

Tabla 16. Resultados estadísticos UPK full vs full

5.3.2. Análisis de la curva ROC Full vs Full

A continuación se presenta el estudio de la curva ROC de la figura 48.

- Para el caso del sensor FPC se puede contemplar una linealidad bastante baja y un punto de curvatura máximo elevado, lo que demuestra que la calidad del análisis es alta. El punto máximo de curvatura alcanza un nivel sobre el eje y de aproximadamente 85%.

- Para el caso del sensor NXT, se puede apreciar una calidad en la comparación de muestras y obtención de resultados. En cuanto a la gráfica, la linealidad es muy baja y el punto máximo de curvatura alcanza un valor de aproximadamente el 90% de intentos genuinos aceptados frente a un 15% de intentos impostores aceptados.

- En el caso del sensor UPK se contempla una tendencia, superior al resto, a la esquina superior izquierda, lo que supone una calidad máxima en el análisis. Para valores de más del 90% de usuarios genuinos aceptados, se observa tan sólo un 9 % de intentos impostores aceptados. Por otro lado, es donde se localiza la menor linealidad de todos los sistemas

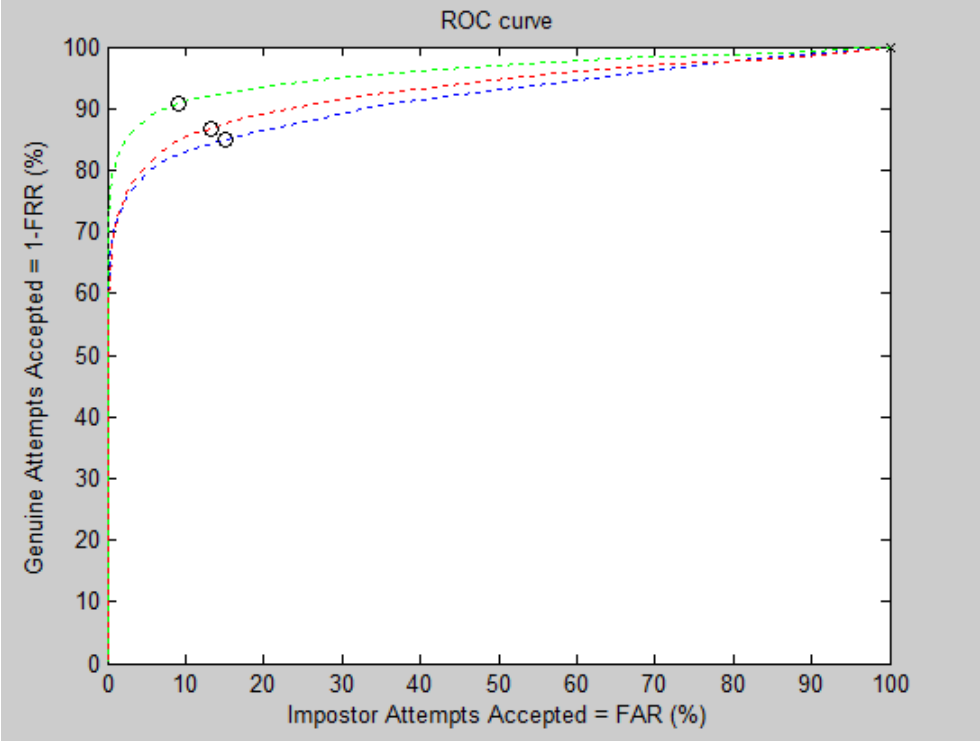

Figura 48. Curva ROC full vs full

AZUL	FPC
ROJO	NXT
VERDE	UPK

5.3.3. Análisis curva DET Full vs Full

- En el caso del sensor FPC, al igual que en la curva ROC, en la curva DET de la figura49 el análisis es más próximo al origen de coordenadas, lo que indica un nivel alto de efectividad y de calidad en la comparación.

- Para el sensor NXT, al igual que en la curva ROC, los resultados obtenidos en la curva DET de la figura 49 muestran una peor calidad para el sistema térmico en comparación con los análisis capacitivos. La línea se centra aún mas respecto al origen y los porcentajes son mucho menores, es decir, frente a un 12 % de falso rechazo, aparece un 12% de falsa aceptación.

- Por último, en el caso del sensor UPK, la curva DET tiene una alta tendencia al origen lo que implica que el análisis es muy exitoso en todas sus pruebas, utilizando imágenes de alta resolución y comparándolas.

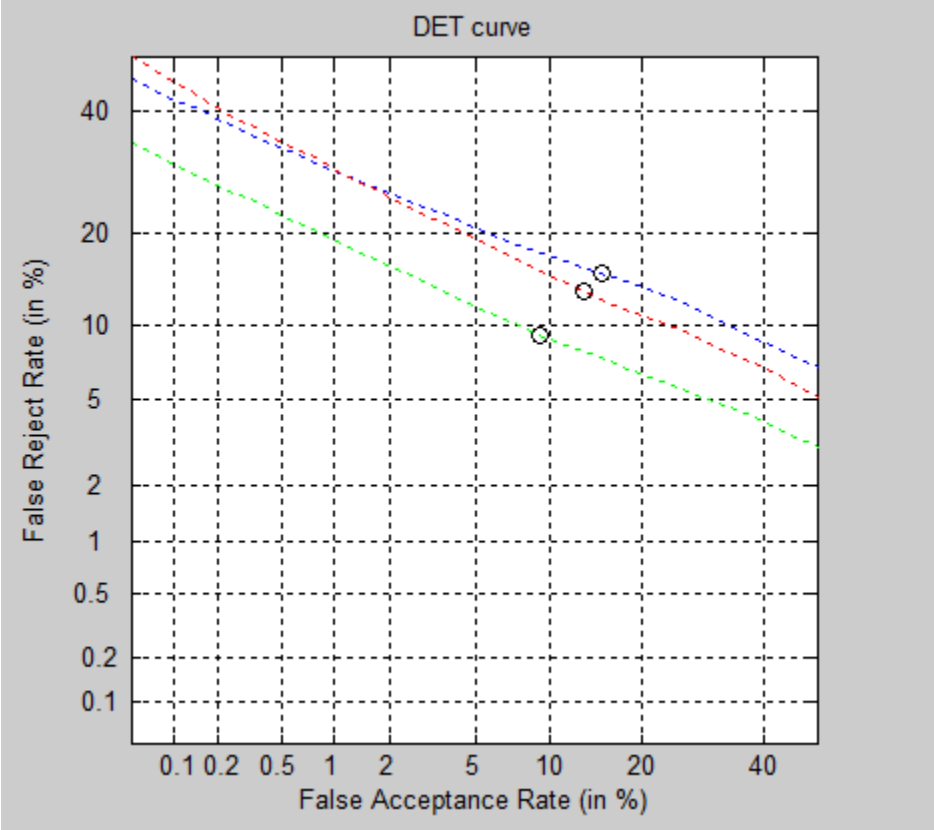

Figura 49.Curva DET full vs full

AZUL	FPC
ROJO	NXT
VERDE	UPK

5.4. Full vs 8x8

5.4.1. FAR vs FRR

Las figuras 50, 51 y 52, muestran las curvas FAR vs FRR para imágenes Full vs 8x8. Como se ha mencionado anteriormente, a medida que disminuye el valor del EER, mejor será el sistema. En esta segunda parte se estudian los sistemas de imágenes completas frente a imágenes recortadas, esto hace que los valores de EER aumenten, mientras que su calidad disminuye. En el análisis de la curva, el algoritmo estadístico ha determinado que el mejor sistema es el UPK full vs 8x8, con un valor de EER de 21,6702, tal y como se muestra en la tabla 19. Seguido muy de cerca por el sensor capacitivo FPC, el cual obtiene un valor de EER de 22,5881, localizado en la tabla 17.

A continuación, se muestra en la figura 50 la curva FAR vs FRR referente al sensor FPC.

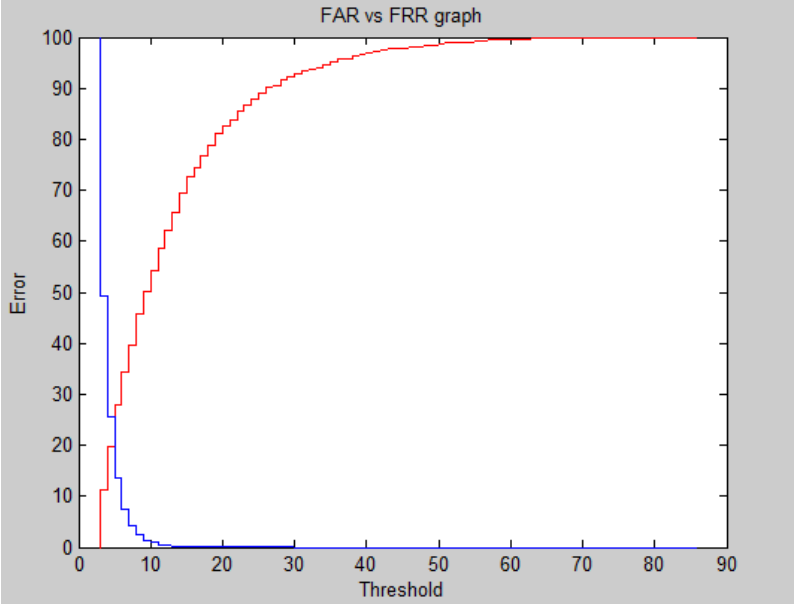

Figura 50. FAR vs FRR FPC full vs 8x8

Donde se consiguen los siguientes valores estadísticos

EER	22.5881
ConfInterEER	0.7507

Tabla 17. Resultados estadísticos FPC full vs 8x8

A continuación, se muestra en la figura 51 la curva FAR vs FRR referente al sensor NXT.

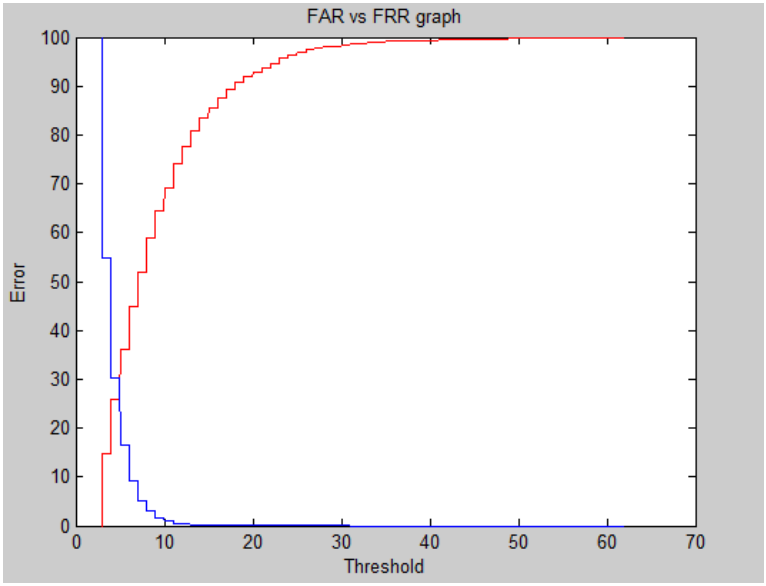

Figura 51. FAR vs FRR NXT full vs 8x8

Donde se obtienen los siguientes valores estadísticos

EER	28.0531
ConfInterEER	0.7244

Tabla 18. Resultados estadísticos NXT full vs 8x8

A continuación se muestra en la figura 52 la curva FAR vs FRR referente al sensor UPK.

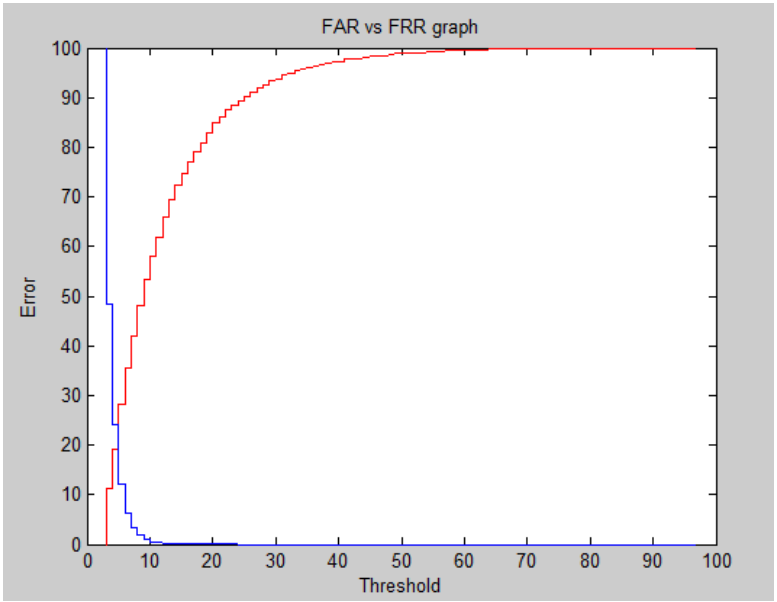

Figura 52. FAR vs FRR UPK full vs 8x8

Donde se alcanzan los siguientes valores estadísticos

EER	21.6702
ConfInterEER	0.7203

Tabla 19. Resultados estadísticos UPK full vs 8x8

5.4.2. Análisis curva ROC Full vs 8x8

En el estudio de la curva ROC de la figura 53 puede establecerse lo siguiente:

- Para el caso del sensor FPC en el sistema full vs 8x8, se utiliza un sensor de alta resolución para el reclutamiento y de uno más pequeño para la identificación. El punto máximo de curvatura está próximo al 75% mucho menor que en el caso de la evaluación Full vs Full. Por otro lado, la curva es más lineal que en el caso del análisis Full vs Full.

- Para el caso del sensor NXT de la figura el punto máximo de curvatura es de aproximadamente el 70%, muy bajo en comparación con la tecnología capacitiva.

- En el caso del sensor UPK, la curva ROC de la figura 53ha disminuido su calidad en gran medida frente al primer análisis Full vs Full. La relación es del 80% de intentos genuinos aceptados, frente a un 20 % de intentos impostores aceptados, en el valor máximo de curvatura. Además, se localiza una curva poco lineal.

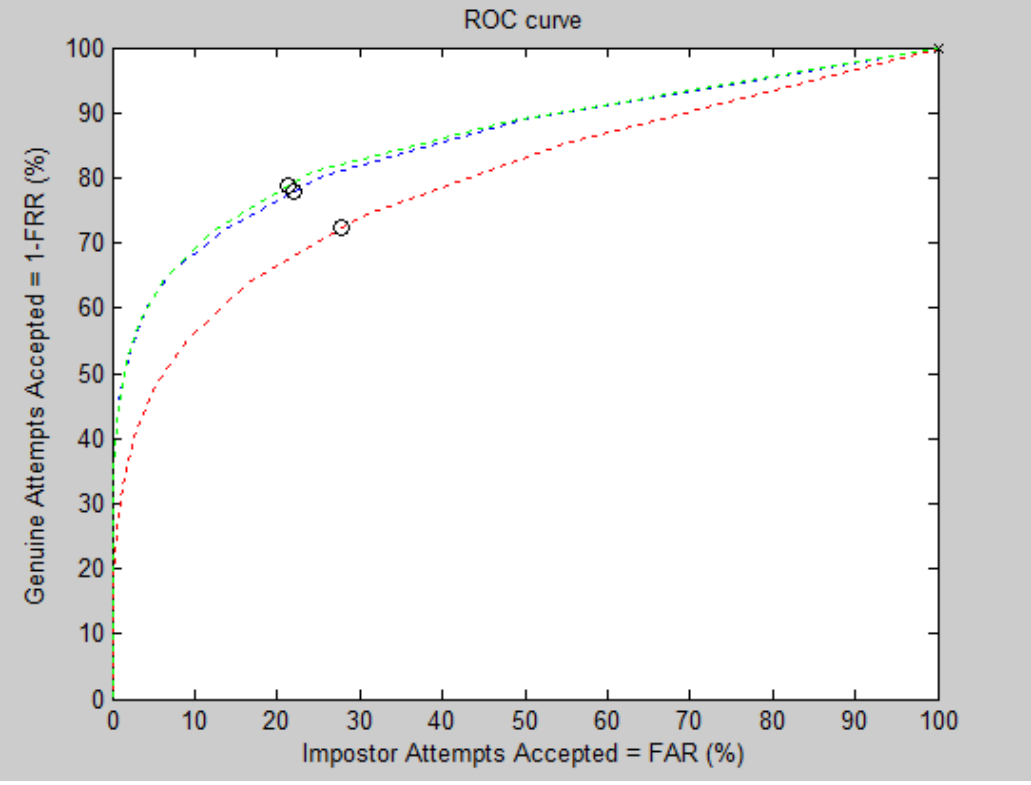

Figura 53. Curva ROC full vs 8x8

AZUL	FPC
ROJO	NXT
VERDE	UPK

5.4.3. Análisis curva DET Full vs 8x8

En el estudio de la curva DET de la figura 54 se observa:

- Para el caso del sensor FPC, la curva DET forma una línea con unos puntos alejados del origen, lo que implica un alto valor en el porcentaje de falsa aceptación, así como un alto valor de porcentaje de falso rechazo. Con estos resultados se asegura que la calidad de las comparaciones es baja-media y que la posibilidad de que el sistema falle es bastante alta.

- Para el caso del sensor NXT, al igual que en la curva ROC continúan apareciendo resultados con un alto porcentaje de rechazo y de falsa aceptación. Esto supone una orientación de la gráfica alejada del origen de coordenadas, tal y como se muestra en la figura54.

- En el caso del sensor UPK forma una línea con unos puntos no alejados del origen, lo que implica un alto valor de veracidad en la comparación de muestras. Con estos resultados se afirma que la calidad de las comparaciones es media-alta y que la posibilidad de que el sistema falle es mucho mayor que en el sistema Full vs Full.

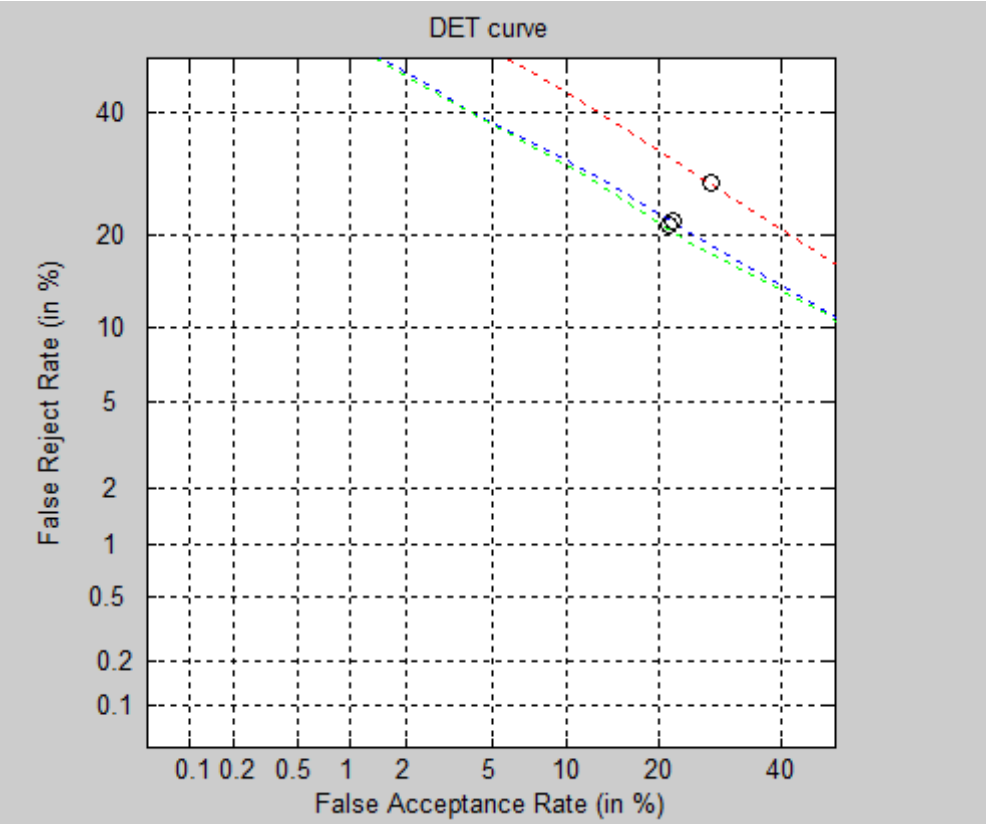

Figura 54. Curva DET full vs 8x8

AZUL	FPC
ROJO	NXT
VERDE	UPK

5.5. 8x8 vs 8x8

5.5.1. FAR vs FRR

Las figuras 55, 56 y 57, muestran las curvas FAR vs FRR para imágenes 8x8 vs 8x8. Como se ha mencionado anteriormente, a medida que disminuye el valor del EER, mejor será el sistema. En esta tercera y última parte se estudian los sistemas de imágenes recortadas, esto hace que los valores de EER aumenten aún más que en la prueba anterior, mientras que su calidad disminuye aún más. En el análisis de la curva, el algoritmo estadístico ha determinado que el mejor sistema es el UPK 8x8 vs 8x8, con un valor de EER de 30,0730 tal y como se muestra en la tabla 22. Seguido muy de cerca por el sensor capacitivo FPC, el cual obtiene un valor de EER de 31,1367, localizado en la tabla 20.

A continuación se muestra en la figura 55 la curva FAR vs FRR referente al sensor FPC.

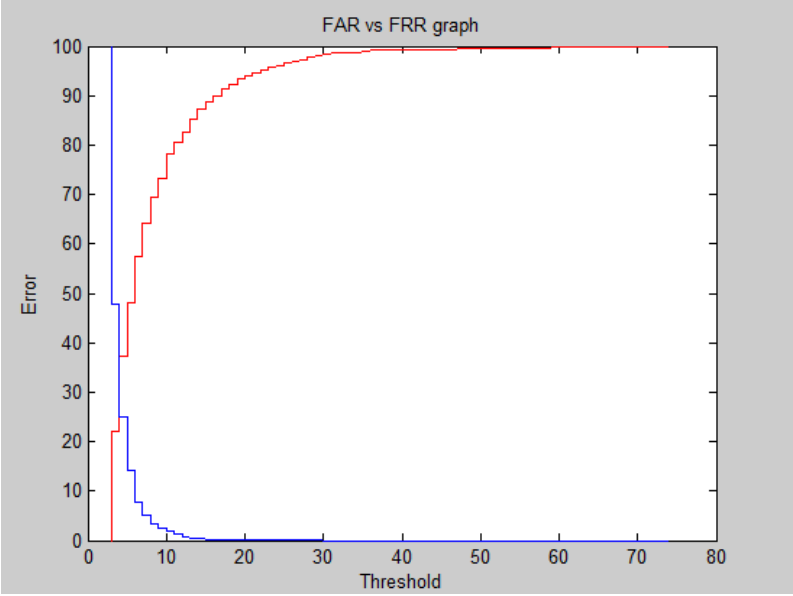

Figura 55. FAR vs FRR FPC 8x8 vs 8x8

Donde se adquieren los siguientes valores estadísticos

EER	31.1367
ConfInterEER	1.1265

Tabla 20.Resultados estadísticos FPC 8x8 vs 8x8

A continuación se muestra en la figura 56 la curva FAR vs FRR referente al sensor NXT.

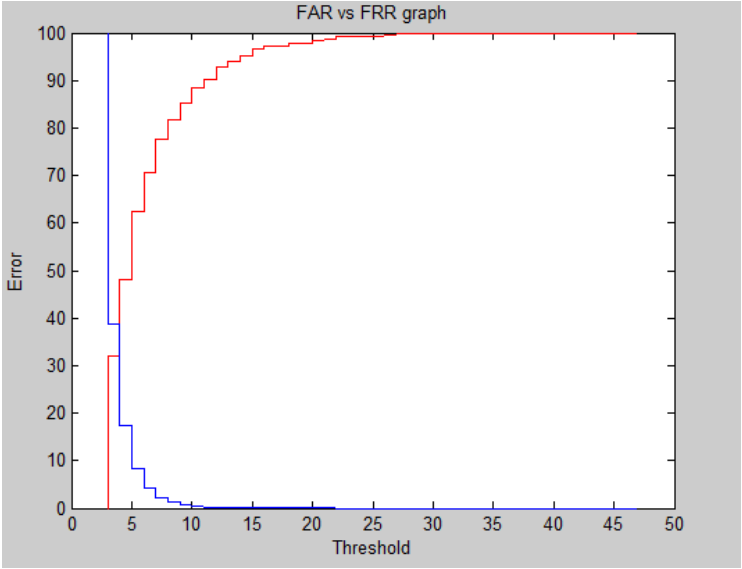

Figura 56.FAR vs FRR NXT 8x8 vs 8x8

Donde se obtienen los siguientes valores estadísticos

EER	35.3580
ConfInterEER	1.3322

Tabla 21.Resultados estadísticos NXT 8x8vs 8x8

A continuación se muestra en la figura 57 la curva FAR vs FRR referente al sensor UPK.

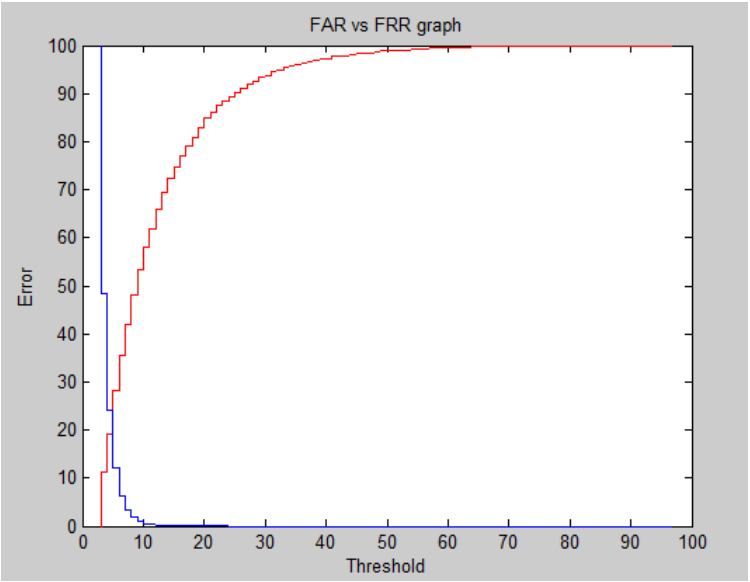

Figura 57.FAR vs FRR UPK 8x8 vs 8x8

Donde se consiguen los siguientes valores estadísticos

EER	30.0730
ConfInterEER	1.4913

Tabla 22.Resultados estadísticos UPK 8x8vs 8x8

5.5.2. Análisis curva ROC 8x8 vs 8x8

En el estudio de la curva ROC de la figura 58 se puede determinar qué:

- Para el caso del sensor FPC, en la figura 58, se tendrá en cuenta la curvatura e inclinación de ésta para determinar su calidad. Como se puede observar, su punto máximo en el centro de la curva no es elevado, de aproximadamente el 68% . Por ello, se determina que la calidad de las comparaciones no es buena. Por otro lado, se encuentra una alta linealidad en comparación con el resto de pruebas.

- Para el caso del sensor NXT, se observa una alta linealidad en la curva obtenida, lo que implica una baja calidad en la comparación. Por otro lado, el punto máximo de curvatura se sitúa en una zona bastante baja, alcanzando porcentajes de aproximadamente un 65 %.

- En el caso del sensor UPK, se aprecia una curvatura con tendencia a la parte superior izquierda por lo que la calidad no es excesivamente mala. Esto se puede deber en parte a la gran cantidad demuestras a comparar que se han tomado en cuenta en el estudio frente al resto de los sensores.

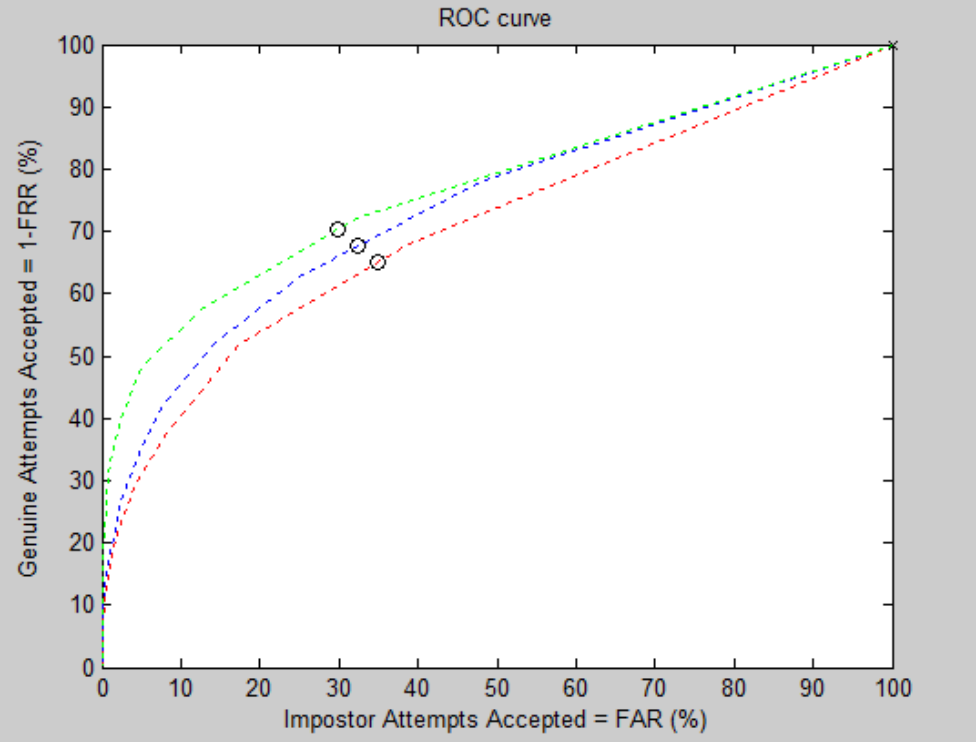

Figura 58.Curva ROC 8x8 vs 8x8

AZUL	FPC
ROJO	NXT
VERDE	UPK

5.5.3. Análisis curva DET 8x8 vs 8x8

En el estudio de la curva DET de la figura 59 se explica que:

- Para el caso del sensor FPC, la gráfica DET impone unos puntos muy alejados del origen lo que implica un alto porcentaje de falsa aceptación, así como un alto porcentaje de falso rechazo. Con estos resultados se asegura que la calidad de las comparaciones es baja y que la posibilidad de que el sistema falle es muy alta. Como conclusión general se puede asegurar que este sistema cometerá bastantes errores en la relación reclutamiento, verificación e identificación. Por ello, se debe proponer un aumento en la cantidad de intentos.

- Para el caso del sensor NXT y al igual que sucedía con el sensor FPC, esta tecnología térmica no es suficiente para alcanzar valores correctos de comparación. Esto supone una gran cantidad de usuarios falsamente rechazados y otros falsamente aceptados. La curva se sitúa a mucha distancia del origen de coordenadas.

- En el caso del sensor UPK, forma una línea con unos puntos no excesivamente alejados del origen. Esto facilita la observación ya que cuenta con unos rasgos positivos en referencia al grado de correcta identificación. Con estos resultados se afirma que la calidad de las comparaciones es media a pesar de que la posibilidad de que el sistema falle es bastante alta.

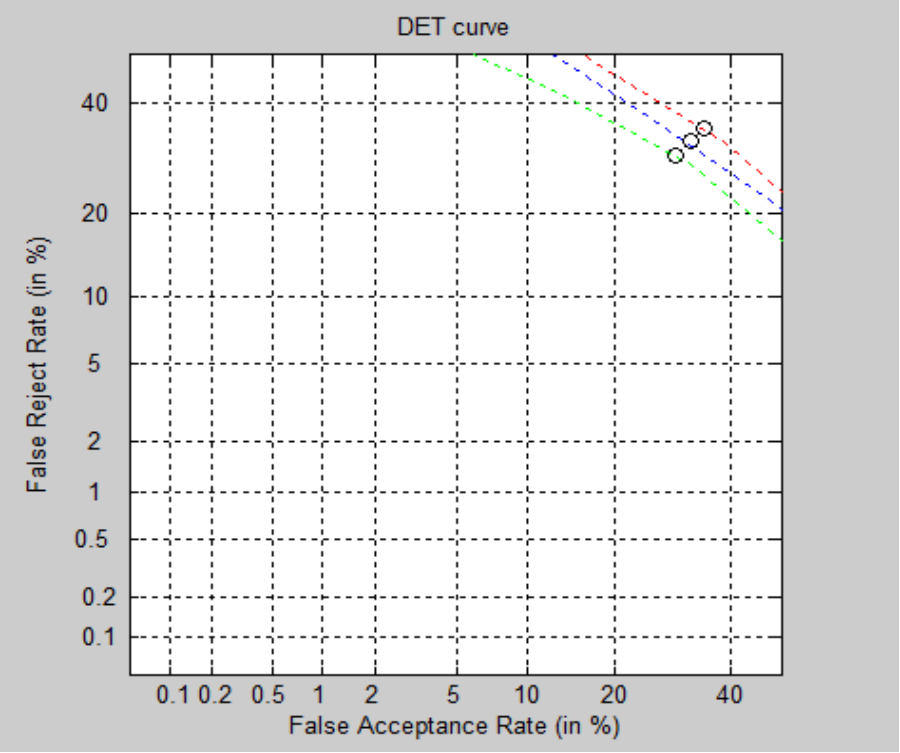

Figura 59.Curva DET 8x8 vs 8x8

AZUL	FPC
ROJO	NXT
VERDE	UPK

6. ANÁLISIS GLOBAL DE RESULTADOS

6.1. Análisis Tiempo de procesado

Una vez obtenidos los resultados de tiempo de procesado se resumen en la tabla 23.

Realizando un estudio comparativo y sin tener en cuenta otros factores como la calidad o el tamaño, se reconoce que el sensor FPC es el más rápido en cuanto a tiempo de procesamiento se refiere. A continuación se encuentran los sensores UPK y el NXT. Uno de los factores más relativos de este estudio es observar como a medida que el tamaño de la huella va aumentando, su tiempo de procesado también lo hace.

Tecnología/Tamaño de imagen	Tiempo Total de procesado
FPC/8x8 vs 8x8	5850 segundos
FPC/Full vs 8x8	11250 segundos
FPC/Full vs Full	5850 segundos
NXT/8x8 vs 8x8	18750 segundos
NXT/Full vs 8x8	18750 segundos
NXT/Full vs Full	98550 segundos
UPK/8x8 vs 8x8	15150 segundos
UPK/Full vs 8x8	30450 segundos
UPK/Full vs Full	93750 segundos

Tabla 23.Tiempo de procesamiento

6.2. Análisis curva ROC

Con el fin de esclarecer una hipótesis en este estudio, se compararán todas las curvas ROC anteriormente descritas. En éstas se ha obtenido un claro sensor y método superior al resto, tal y como se demuestra en la figura 60. Así, es la tecnología capacitiva del sensor UPK mediante la utilización de imágenes de resolución completa Full vs Full, la que mejores resultados obtiene.

La figura 60 muestra la siguiente clasificación:

Sensor	Línea continua	Línea discontinua (.)	Línea discontinua (-)
FPC	Full vs Full	Full vs 8x8	8x8 vs 8x8
NXT	Full vs Full	Full vs 8x8	8x8 vs 8x8
UPK	Full vs Full	Full vs 8x8	8x8 vs 8x8

Tabla 24.Tiempo de comparación Full vs Full UPK

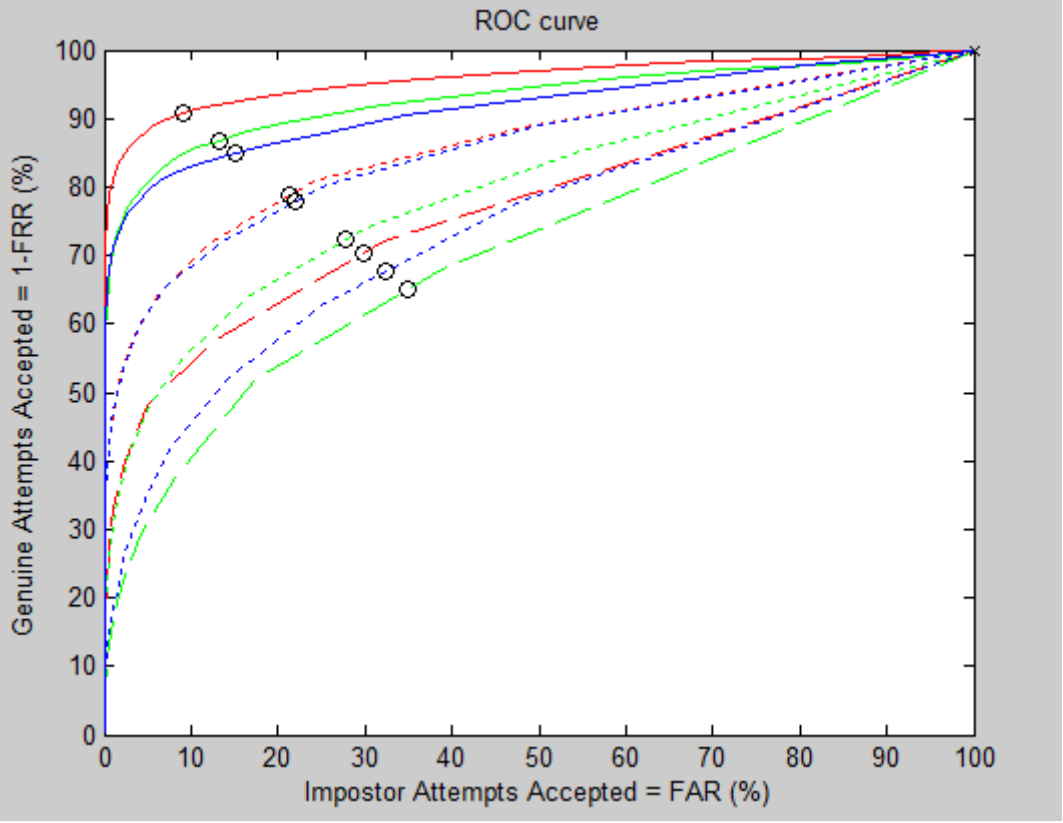

Figura 60.Curva ROC global

6.2.1. Análisis comparativo 8x8 vs 8x8

Se organizará un estudio comparativo dependiendo del tamaño de la muestra a reclutar. Comienza con el análisis 8x8 vs 8x8.

En este caso, los mejores resultados se localizan con el sensor UPK, el cual alcanza valores por encima del 65 % frente a los 64% del FPC o 60% del NXT. Todas las curvas muestran la misma lógica, una secuencia de puntos muy lineal con cierta tendencia a la esquina superior izquierda, pero con unos porcentajes demasiado bajos. Para estas muestras, el estudio no asegura una correcta implementación de ninguno de los tres sensores ya que estos serán fácilmente accesibles.

Como posibles ejemplos de uso, está el acceso a un teléfono móvil que cuente con un sensor ya sea en la propia pantalla, cubierta o detrás de éste, tal y como se representa en la figura 61. Se usaría el mismo dispositivo para el registro que para la identificación y el tamaño del sensor no debe ser mayor que el espacio delimitado por una imagen de tamaño 8x8.

Con el fin de mejorar el sistema, se podría aumentar la cantidad de dedos a posicionar.

Figura 61.Móvil con tecnología de identificación biométrica [34]

6.2.2. Análisis de resultados Full vs 8x8

Para el caso actual de imágenes de reclutamiento *Full* frente a muestras de verificación 8x8, se puede especificar que ambos sensores capacitivos obtienen mejores resultados que el térmico. Llegan a alcanzar aproximadamente el valor del 80 % de usuarios genuinos aceptados frente al 20 % de intentos de usuarios impostores aceptados.

Ambas curvas muestran una actitud muy poco lineal lo que muestra un comportamiento muy positivo en ambos sistemas, con tendencia hacia la esquina superior izquierda. Este tipo de sistemas ofrecen una ventaja y es que el reclutamiento puede ser realizado con un sensor de alta resolución de gran tamaño. Mientras, la verificación se puede realizar con uno más pequeño situado en cualquier zona del dispositivo o sala al que se quiera acceder. Es uno de los resultados más positivos del estudio en cuanto a funcionalidad, usabilidad y calidad de la comparación. Este sistema puede ser utilizado para el registro en cualquier base de datos y posterior verificación de manera generalizada. Algunas posibles funcionalidades son, el acceso a recintos deportivos o con una elevada seguridad, pago con teléfono móvil mediante tecnología Radio Frequency IDentification (RFID) con verificación de huella dactilar.

6.2.3. Análisis comparativo Full vs Full

Como se puede observar, para el caso del análisis Full vs Full, el sensor UPK es el que obtiene un mejor resultado tras las comparaciones, con un porcentaje de aproximadamente un 90% de intentos genuinos aceptados, frente al 86% del sensor NXT o el 84 % del FPC.

En cuanto a las curvas, todas muestran un patrón similar con puntos secuencialmente localizados y con una muy alta tendencia hacia la esquina superior izquierda. Para este tipo de muestras, al contrario que con las 8x8 vs 8x8, el trabajo fin de grado (TFG) asegura una implementación positiva en la práctica. El análisis Full vs Full cuenta con las ventajas de la calidad en la comparación, en este caso muy alta y positiva, siempre y cuando el espacio disponible para este sensor sea el adecuado.

Como posible ejemplo de uso, la posibilidad de acceder a un ordenador de sobremesa que cuente con un sensor de estas de gran tamaño. Se usaría el mismo dispositivo para el registro que para la identificación. Al contrario que con otros sistemas, con tan sólo un dedo se podrían obtener altos niveles de autentificación de usuario genuino. Por todo ello el número de intentos podría ser menor que en el caso de la resolución 8x8.

6.3. Análisis curva DET

Al igual que en el sistema ROC, el sistema DET de la Figura 62 da a mostrar unos resultados de calidad en la comparación de las muestras idénticos siendo:

- Full vs Full: Upk como tecnología y sensor principal.
- Full vs 8x8: Upk o FPC indistintamente como tecnología a utilizar
- 8x8 vs 8x8: Upk como tecnología a utilizar.

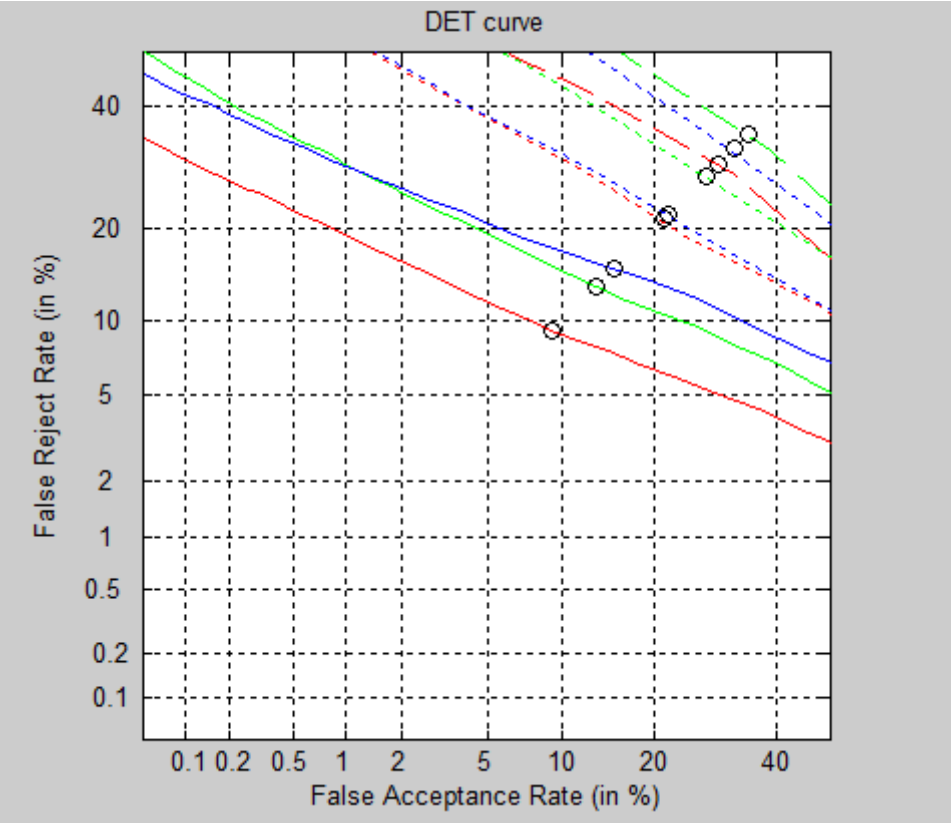

Figura 62.Curva DET global

7. CONCLUSIONES Y LINEAS FUTURAS

En el presente capítulo se exponen las conclusiones generales del TFG. Inicialmente se resumen los objetivos principales del TFG y la explicación de cómo se han desarrollado. A continuación se encuentra un breve resumen de los resultados más relevantes. Finalmente se proponen futuras líneas de investigación que puedan complementar el siguiente estudio.

7.1. Conclusiones generales

A continuación, se presentan las conclusiones generales que han sido obtenidas a partir de la realización de este TFG.

Por un lado se ha conseguido analizar la influencia del tamaño de las imágenes de huellas dactilares, y así se ha conseguido determinar el rendimiento de cada uno de los sistemas de reconocimiento biométrico. Por otro lado, este estudio expuso diferentes posibilidades prácticas, lo que supone una vía para el desarrollo de productos y/o aplicaciones Además, se consiguió optimizar las aplicaciones, lo que supuso una disminución considerable del tiempo de procesado.

7.2. Conclusiones de resultados

En este trabajo se han creado dos aplicaciones cuyo objetivo común era el de generar un análisis estadístico que permitiese conocer la influencia del tamaño de las muestras en el análisis de un sistema biométrico. En concreto, en este trabajo se ha realizado un análisis biométrico basado en el análisis de la huella dactilar. Este estudio nos permite generar datos veraces y determinar qué tipo de tecnología y que tamaño de muestra son las ideales para cada tipo de aplicación práctica. Las conclusiones más relevantes que se pueden extraer del desarrollo de este trabajo de fin de grado son que:

- La tecnología capacitiva desarrollada por el sistema UPK es la más precisa para cualquier tamaño de imagen.
- La utilización de sensores 8x8 es fiable si se incrementa el número de pruebas para la verificación o si aumentan la cantidad de sensores y por tanto el número de muestras a estudiar.
- La implementación de sensores Full vs 8x8 es muy positiva en relación a solo la utilización de 8x8, ya que aumenta la seguridad en las pruebas.
- El uso de imágenes a tamaño completo de las muestras es muy seguro así como no es necesario un gran número de pruebas para la correcta verificación. Sin embargo cuentan con el aspecto negativo del tamaño.

Durante su desarrollo han surgido algunos problemas. Principalmente surgen de la optimización y depuración de código. Gracias a los recursos disponibles en la web y en la biblioteca, se consiguió

optimizar al máximo ambas aplicaciones para generar los resultados. Gracias a las decisiones de diseño, mejora en el acceso a la ruta de las imágenes y eliminación de recursos no útiles durante el proceso de ejecución, se ha conseguido obtener una aplicación fiable y fluida para la obtención de resultados.

Con todo, se considera que un trabajo como el realizado puede ser utilizado como fuente de información principal para una implementación práctica, ya sea para el acceso a determinados espacios con una seguridad alta o la identificación de usuarios en telefonía móvil.

7.3. Líneas futuras

Se considera que este trabajo puede inspirar futuras líneas de investigación. Por ejemplo, como posible mejora para el futuro y más concretamente en el campo de la telefonía móvil, proponemos el estudio de la implementación de varios sensores, uno para cada dedo, que trabajen conjuntamente y cuyos resultados puedan determinar de manera más exacta al usuario. Igualmente, sería interesante el estudio de la aplicación de esta tecnología como sistema global de identificación.

Sería interesante la implementación de este análisis con huellas capturadas directamente por un sensor de tamaño reducido, en lugar de utilizar la imagen recortada. Realizando una comparación de ambos sistemas, se podría determinar definitivamente la validez de la evaluación.

BIBLIOGRAFÍA

1. ISO/IEC 19795-6:2012, de 1 de Febrero de 2012, de Biometric performance testing and reporting. ISO/IEC JTC 1/SC 37 **[1]**

2. España.Ley Orgánica 15/1999, de 14 de Diciembre de 1999, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 14 de Enero de 2000, núm. 298 **[2]**

3. Wikipedia*: Biometría* [en línea]. [Consulta: 1 de septiembre 2015]. Disponible en: https://es.wikipedia.org/wiki/Biometr%C3%ADa **[3]**

4. SÁNCHEZ AVILA, Carmen, "*Aplicaciones de la Biometría a la seguridad"*. Universidad Politécnica de Madrid, Grupo de Biometría, Bioseñales y Seguridad Centro de Domótica Integral: Biometría, p.6. [Consulta: 1 septiembre 2015] .Disponible en: http://www.criptored.upm.es/descarga/TASSI2012_CarmenSanchez.pdf **[4]**

5. *Hablemos de biometría. La biometría como única forma segura de identificación de las personas* [en línea]. Umanick: Ventajas y desventajas, 14. [Consulta: 25 agosto 2015]. Disponible en : http://es.slideshare.net/umanick/hablemos-de-biometra-la-como-biometra-nica-forma-segura-de-identificacin-de-las-personas [**5]**

6. *Clasificación de los Sistemas* biométricos[en línea]. UNAM-Facultad de ingeniería biometría informática: *Capítulo 3.1*"Por su tipo".[Consulta: 3 septiembre 2015].Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/clasificaciontipo.html **[6]**

7. SÁNCHEZ AVILA, Carmen, "*Aplicaciones de la Biometría a la seguridad"*. Universidad Politécnica de Madrid, Grupo de Biometría, Bioseñales y Seguridad Centro de Domótica Integral: Biometría, p.5. [Consulta: 1 septiembre 2015] .Disponible en: http://www.criptored.upm.es/descarga/TASSI2012_CarmenSanchez.pdf **[7]**

8. *Área de conocimiento* [en línea]. Kimaldi: Verificación e identificación biométrica.[Consulta: 01 septiembre 2015]. Disponible en: http://www.kimaldi.com/area_de_conocimiento/biometria/verificacion_e_identificacion_biometrica **[8]**

9. *¿Qué es la biometría?* [en línea]. Fingertech: Verificación.[Consulta: 3 septiembre 2015]. Disponible en: http://www.fingertech.com.ar/Control-RRHH-Empleados/Huella-Digital/Que-es-biometria-huella-digital.asp **[9]**

10. GALTON, Francis, "Finger Prints". Galton [Consulta : 27 Agosto 2015] .Disponible en: http://galton.org/fingerprinter.html **[10]**

11. Wikipedia*: Huella Dactilar* [en línea]. [Consulta: 1 de septiembre 2015]. Disponible en: https://es.wikipedia.org/wiki/Huella_dactilar **[11]**

12. *Acerca de la* Biometría [en línea] . Biometría: Historia de la biometría. [Consulta: 25 agosto 2015] Disponible en: http://www.biometria.gov.ar/acerca-de-la-biometria/historia-de-la-biometria.aspx **[12]**

13. BAEZ MOYANO, Luciano Martín, *1*, Extracción de características de Galton de Huellas Dactilares por procesamiento digital de la imagen, http://www.cneisi.frc.utn.edu.ar/papers/736ea8ecf9f30f83571ddd6d4412.pdf **[13]**

14. Emol Tecnología. "Investigadores crean método para determinar la antigüedad de una huella dactilar". Tecnología,2014 , Disponible en: http://www.emol.com/noticias/tecnologia/2014/06/04/663662/investigadores-crean-metodo-para-determinar-la-antiguedad-de-una-huella-dactilar.html **[14]**

15. SALZA, Cesar. *Nueva tecnología permitirá pantallas enteras con sensor de huella* [en línea]. Industria de la Tecnología , [Consulta: 26 Agosto 2015]. Disponible en: http://www.cnet.com/es/noticias/nueva-tecnologia-permitira-pantallas-enteras-con-sensor-de-huella/ **[15]**

16. PASCUAL, Juan Antonio. *Las nuevas contraseñas biométricas: tu cuerpo es la clave* [en línea]. [Consulta: 30 Agosto 2015]. Disponible en: http://computerhoy.com/noticias/hardware/nuevas-contrasenas-biometricas-tu-cuerpo-es-clave-11789 **[16]**

17. RINALDI, Camila. *Análisis preliminar del Sony Xperia Z5: Pocas pero interesantes mejoras* [en línea].Consulta: 30 Agosto 2015]. Disponible en: *http://www.androidpit.es/sony-xperia-z5-analisis* **[17]**

18. PUERTO, Kote. *HTC One Max* [en línea].Consulta: 29 Agosto 2015]. Disponible en: http://www.xataka.com/moviles/htc-one-max **[18]**

19. Wikipedia*: Sensor de huella digital* [en línea]. [Consulta: 5 de septiembre 2015]. Disponible en: https://es.wikipedia.org/wiki/Sensor_de_huella_digital **[19]**

20. Product Sheet: *Fingerprints* [en línea]. [Consulta: 2 septiembre de 2015]. Disponible en: http://www.fingerprints.com/wp-content/uploads/2013/08/720-FPC1011F3_A_Product-sheet.pdf **[20]**

21. NEXT Biometrics Group ASA. [en línea]. [Consulta :26 agosto 2015]. Disponible en: http://www.marketwired.com/press-release/next-biometrics-receives-us-order-fingerprint-sensors-follows-recent-us-order-next-fingerprint-oslo-next-2047110.htm **[21]**

22. Product Sheet: *Eikon Touch* [en línea]. [Consulta: 2 septiembre de 2015]. Disponible en: http://www.siasa.com/productos/documentos/EikonTouch.pdf **[22]**

23. WATSON, Craig, GARRIS, Michael, TABASSI, Elham , WILSON, Charles , MCCABE, Michael, JANET,Stanley , KO,Kenneth ,*48-61*, User's Guide to NIST Biometric Image Software, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51097 **[23]**

24. WATSON, Craig, GARRIS, Michael, TABASSI, Elham , WILSON, Charles , MCCABE, Michael, JANET,Stanley , KO,Kenneth ,*14 -16*, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51096, [**24]**

25. BioSecure Tool. *Performance Evaluation of a biometric verification system, p. 1-3.* **[25]**

26. Wikipedia*: Microsoft Visual Studio* [en línea]. [Consulta: 3 de septiembre 2015]. Disponible en: https://es.wikipedia.org/wiki/Microsoft_Visual_Studio **[26]**

27. Wikipedia*: C Sharp* [en línea]. [Consulta: 4 de septiembre 2015]. Disponible en: https://es.wikipedia.org/wiki/C_Sharp **[27]**

28. Wikipedia*: MatLab* [en línea]. [Consulta: 4 de septiembre 2015]. Disponible en: https://es.wikipedia.org/wiki/MATLAB **[28]**

29. NIST. *NIST Biometric Image Software* [en línea]. Information Technology Laboratory. [Consulta: 23 Septiembre 2015].Disponible en: http://www.nist.gov/itl/iad/ig/nbis.cfm **[29]**

30. Wikipedia*: Curva ROC* [en línea]. [Consulta: 4 de septiembre 2015]. Disponible en: https://es.wikipedia.org/wiki/Curva_ROC **[30]**

31. Hospital Universitario Ramón y Cajal. *Tipos de curva ROC y su clasificación.*[Consulta: 20 Agosto 2015]. Disponible en: www.hrc.es/bioest/roc_1.html **[31]**

32. Scientific Software Solution. *Características curvas ROC.*[Consulta: 17 Agosto 2015]**.** Disponible en: *www.scientificsoftware-solutions.com* **[32]**

33. Wikipedia*: Detection Error Tradeoff* [en línea]. [Consulta: 4 de septiembre 2015]. Disponible en: *https://en.wikipedia.org/wiki/Detection_error_tradeoff* **[33]**

34. Androidsis. *Sensor de huellas dactilares: Los usuarios que tengan unsmartphone con sensor de huellas dactilares tienen menor protección jurídica en Estados Unidos.*[Consulta: 10 septiembre 2015].Disponible en*: http://www.androidsis.com/sensor-de-huellas-dactilares* **[34]**

ANEXO 1: Presupuesto y Planificación del trabajo

Con el fin de poder conocer el cálculo aproximado del coste del Trabajo Fin de Grado, inicialmente se procede a la descomposición de todas las tareas que se han realizado en horas trabajadas.

A1. Planificación

Bloque 1: Documentación Inicial

Estudio de la plataforma Visual Studio 2013 (20 horas)

Estudio de la plataforma MatLab (15 horas)

Búsqueda de información y tutoriales acerca de la programación en lenguaje C Sharp (30 horas)

Búsqueda de diversa información acerca de la aplicación en consola y WPF (7 horas)

Bloque 2: Desarrollo de la aplicación

Actividad principal (20 horas)

Actividad de registro (10 horas)

Actividades secundarias (10 horas)

Interconexión de actividades (25 horas)

Bloque 3: Análisis y obtención de resultados

Comparación de muestras (80 horas)

Obtención de resultados (10 horas)

Análisis de resultados (10 horas)

Bloque 4: Elaboración de la memoria

Redacción de la memoria (60 horas)

Corrección y maquetación (10 horas)

FASES	HORAS EMPLEADAS
B1. Documentación Inicial	72
B2. Desarrollo de la aplicación	65
B3. Análisis y obtención de resultados	100
B4. Elaboración de la memoria	70
TOTAL	**307 horas**

Tabla 25.Tiempo total utilizado

A2. Presupuesto del Trabajo Fin de Grado

A2.1. Coste del material

Para la correcta resolución del Trabajo Fin de Grado, han sido necesarios 1 ordenador, de altas prestaciones para el desarrollo de la aplicación en Visual Studio y la generación de resultados de manera eficiente, así como la bonificación que tenía el realizar el estudio. Considerando un periodo de amortización de cada uno de los dispositivos de 4 años y tomando en consideración el tiempo del proyecto, se redactan los costes según la Tabla 26.

CONCEPTO	PRECIO
Ordenador de altas prestaciones	200
Bonificación usuarios	675
TOTAL	**875**

Tabla 26.Coste total de material

A2.2. Coste del personal

Para la consecución del proyecto ha sido fundamental la presencia de un jefe de proyecto y un ingeniero.

OCUPACIÓN	HORAS	PRECIO/HORA	IMPORTE(€)
DIRECTOR	5	90	450
JEFE DE PROYECTO	10	60	600
INGENIERO	307	30	9210
TOTAL	487	-	10260

Tabla 27.Coste total de personal

A2.3. Coste Total

CONCEPTO	PRECIO(€)
Coste de materiales	875,00
Coste de personal	10260,00
Costes indirectos (20%)	2227,00
Subtotal	12487,00
IVA (21%)	2622,27
TOTAL	15109,27 **€**

Tabla 28.Coste total

El coste total del proyecto es de Quince mil ciento nueve euros con veintisiete céntimos.

Leganés, 25 de Septiembre de 2015

El ingeniero